瑞星杀毒软件中小企业版
中文使用手册

北京瑞星科技股份有限公司

公司简介

北京瑞星科技股份有限公司是以研究、开发、生产及销售计算机反病毒产品和网络安全产品的高新技术企业。公司成立于 1991 年 11 月，位于中国的“硅谷”——北京中关村，是享誉全国的资深计算机安全公司。公司现有研发部、销售部、技术服务部、市场推广部、网络信息部、生产部等十个部门。拥有近百名由博士、硕士、学士及大专毕业人员组成的高素质专业人才队伍。

瑞星杀毒软件是瑞星公司针对各种流行于国内外危害较大的恶性计算机病毒和“黑客”程序，自主研制开发的病毒检测和清除工具。产品有适用于DOS、Windows 9x/Me/2000/NT/XP等操作系统平台的【单机版】、适用于Windows NT/2000网络环境的**【中小企业版】**和适用于UNIX、LINUX环境的【中小企业版】。此外，在网络安全领域，瑞星的网络防火墙、入侵检测和漏洞扫描等产品也将为用户的网络安全提供强大技术解决方案。瑞星产品先后荣获 “国家级科技成果奖”、“国家重点新产品”奖，并被国家科委列入1998年国家级“火炬计划”项目。

瑞星公司的宗旨是让所有用户的计算机系统都能得到最可靠的保障，同时享受周到、完善、便捷的服务。通过近十年的发展，公司已拥有庞大的销售网络和完备的客户服务体系，市场占有率遥遥领先。已经成为国内规模最大，技术实力最强，市场和服务体系最完整、最规范的计算机反病毒和网络安全企业。瑞星在企业稳固发展的基础上，坚持不懈地投身于计算机反病毒事业，为电脑与网络信息的安全作出了应有的贡献。

重要声明

请在使用瑞星杀毒软件之前认真阅读配套的使用手册，当您开始使用瑞星杀毒软件时，瑞星公司认为您已经阅读了本使用手册。

本使用手册为瑞星杀毒软件中小企业版的使用手册，其内容将随着瑞星杀毒软件的更新换代而改变，恕不另行通知。从瑞星网站可下载本使用手册的最新版。

请在购买软件后一周内，认真填写“**用户注册卡**”并邮寄到瑞星公司技术服务部进行登记注册（注：不能在瑞星网站注册!）。注册后的产品才会得到唯一合法使用该套产品的“产品授权书”，其中包括用于从瑞星网站下载升级的“用户 ID 号”。对于自购买日起一个月后未持有“产品授权书”的使用者，瑞星公司有权拒绝提供升级程序、技术支持和售后服务。并对因未及时获得瑞星的产品、技术、病毒疫情和服务信息造成的影响不承担任何责任。了解注册用户获得的服务，请参阅《客户服务指南》或注册后收到“致瑞星用户的信”和“计算机防病毒安全服务意向书”。

作为计算机病毒清除工具，杀毒软件将进行不断的升级。无论是功能的增加、性能的提高，还是清除病毒种类的增加都关系到其实际的使用价值。所以，在使用本产品过程中应随时保持与瑞星公司的联系，以及时获得升级程序或更新换代产品。

感谢您购买瑞星公司出品的瑞星杀毒软件系列产品。

目录

第一章 认识瑞星杀毒软件中小企业版

1.1 产品组成

当您通过合法途径获得瑞星杀毒软件中小企业版的使用权后，在安装使用前，请仔细检查核对包装内的组件：

1. 光盘：包含瑞星杀毒软件中小企业版所有程序。
2. 磁盘：随中小企业版赠送的瑞星杀毒软件〖DOS 盘〗。
3. 《使用手册》：即本手册，通过阅读它，掌握本软件的详细使用方法和技巧。
4. 《客户服务指南》：本指南将帮助用户获得相应的技术支持和服务。
5. 用户注册卡：用于确认用户合法使用本套软件的合法资格（注：在打开包装后，请填写并挂号寄回瑞星公司技术服务部）。
6. 回寄信封：用于邮寄“用户注册卡”。
7. 产品序列号：为本套产品分配的唯一身份证明，缺少它，本软件将无法安装。（注：产品序列号见本手册封二和“用户注册卡”）

1.2 主要文件清单

系统光盘

序号	文件名	说　明
1	RavSetup.exe	瑞星杀毒软件中小企业版安装程序
2	Ravscript.exe	脚本登录安装程序
3	RavCheck.exe	瑞星杀毒软件中小企业版辅助安装程序
4	Autorun.inf	光盘自启动配置文件
5	Handbook	安装及使用说明书
6	Autorun.exe	光盘自动运行程序

DOS 盘杀毒软件

序号	文件名	说　明
1	Rav.exe	瑞星杀毒软件〖DOS 盘〗运行程序
2	Virus.def	DOS 盘病毒库
3	Ravdos.exe	硬盘修复程序
4	Mouse.com	鼠标驱动程序
5	其他	用于启动计算机并保障计算机正常运行

1.3 应用网络环境

瑞星杀毒软件【网络版】是专门为 Windows NT/2000 网络环境开发的计算机病毒防护系统。经过瑞星公司员工的不断努力，【网络版】由最初的一套支持中小规模网络的防病毒产品，发展为一个产品系列，其中包括：

(1) 企业版：支持各种复杂网络环境的网络版，它可以支持多级控制、多级升级和多级查杀毒。

(2) 中小企业版：瑞星公司为中小企业量身定制的一套防病毒产品，它是【企业版】的一个子集，不支持多级控制功能。同时，它所支持的客户端和服务器端的总数不超过 200 个。

(3) 专用版：瑞星公司为特殊行业、特殊地区定制的一类防病毒产品。根据不同用户的需要，对【企业版】的功能做了一些调整。不同的专用版，功能是不同的。

瑞星杀毒软件中小企业版所能够适应的平台包括：

- 它支持的服务器操作系统有：
  - Windows NT Server 4.0 简体中文版,英文版
  - Windows 2000 Server 简体中文版,英文版
  - Windows 2000 Advanced Server 简体中文版,英文版
- 它支持的客户机操作系统有：
  - Windows 95/98/me/xp 简体中文版,英文版
  - Windows NT Workstation 4.0 简体中文版,英文版
  - Windows 2000 Professional 简体中文版,英文版
  - Windows XP Professional 简体中文版,英文版

第二章 中小企业版概述

2.1 瑞星杀毒软件中小企业版体系结构

瑞星杀毒软件中小企业版整个防病毒体系是由四个相互关联的子系统组成。每一个子系统均包括若干不同的模块，除承担各自的任务外，还与另外子系统通讯，协同工作，共同完成对网络的病毒防护工作。

一、系统中心

系统中心是整个瑞星网络防病毒系统的信息管理和病毒防护的自动控制核心。它实时地记录防护体系内每台计算机上的病毒监控、检测和清除信息。同时，根据管理控制台的设置，实现对整个防护系统的自动控制。其他子系统只有在系统中心工作后，才可实现各自的网络防护功能。它必须先于其它子系统安装到符合条件的服务器上。详细内容，请参阅第三章“系统中心的安装”。

二、服务器端

服务器端是专门为可以应用为网络服务器的操作系统设计的防病毒子系统。

三、客户端

客户端是专门为网络工作站（客户机）设计的防病毒子系统。它承担着对当前工作站上病毒的实时监控、检测和清除任务，同时自动向瑞星系统中心报告病毒监测情况。

四、管理控制台

管理控制台是为网络管理员专门设计，对瑞星网络防病毒系统进行设置、使用和控制的操作平台。利用管理控制台可以集中管理网络上所有已安装过瑞星中小企业版客户端的计算机，保障每个纳入瑞星防护网络的计算机时刻处于最佳的防病毒状态。它既可以安装到服务器上也可以安装到客户机上，视网络管理员的需要，可自由安装。所以，它又被称为“移动管理控制台”。

2.2 瑞星杀毒软件中小企业版是怎样工作的

瑞星杀毒软件中小企业版安装到服务器和客户机上后，通过“系统中心”、“服务器端”、“客户端”和“管理控制台”四个子系统的协同工作，实现了对网络上病毒的实时监控、定时扫描、手动扫描、自动或手动升级、信息管理等功能。同时提供了用户合法身份认证结构，保障用户利益。（如图 1）

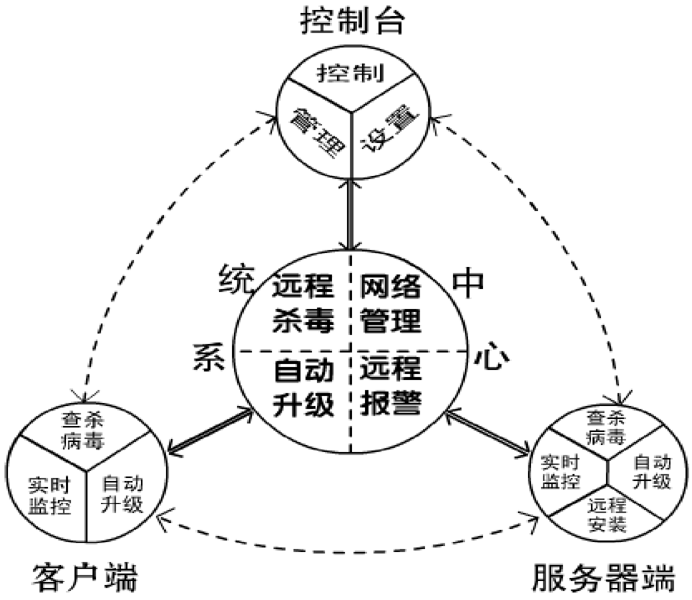


图 1

2.3 如何进行防病毒管理

当一个计算机网络安装瑞星杀毒软件中小企业版后，必须将防病毒管理纳入日常工作。只有通过网络系统管理员、瑞星杀毒软件中小企业版和瑞星公司的技术支持三方努力下才能真正实现整个网络安全的目的。针对瑞星杀毒软件中小企业版提供的功能和特点，建议网络系统管理员进行如下的管理：

➢ 确立病毒防护原则

在通过瑞星杀毒软件中小企业版、企业自身技术人员（多指网络管理员）和瑞星技术支持工程师建立起网络的防病毒体系后，还必须确立该体系运转的工作原则。视每个企业的网络状况、技术人员状况和其他实际情况，瑞星提出以下建议：

- ❖ 所有计算机均应安装瑞星杀毒软件，避免形成防护体系的薄弱环节。在购买产品时，【中小企业版】授权安装的服务器和客户机数量应大于或等于实际的数量。
- ❖ 强制每台计算机开启瑞星实时监控功能。
- ❖ 在每台服务器和客户机上设定合理的定时扫描频率。
- ❖ 每次手动查杀病毒时，选择扫描所有文件。
- ❖ 在重要服务器或客户机上选定【清除之前备份带毒文件】功能。
- ❖ 系统管理员通过管理控制台获得某台服务器或客户机染毒信息后，应针对该计算机进行专门处理。
- ❖ 和瑞星公司联系进行定期的反病毒培训。

➢ 病毒防护信息管理

系统中心对防护体系内所有计算机的病毒监控、检测，以及处理情况均有记录。对这些信息的有效监控、利用和管理会使整个防病毒工作更加有效。网络管理员应根据网络的实际运行状况和工

作需要制定切实可行的管理方案。

➢ 监控、检测和清除病毒

该项管理是网络防病毒管理的核心，利用瑞星杀毒软件中小企业版提供的各项功能可实现对所有计算机设计具体的管理方案。如，对实时监控、扫描、清除时间、周期等设置。

➢ 未知病毒侦测管理

由于新病毒的不断出现，反病毒软件也要随之更新。只有建立一套完整可行的新病毒侦测和捕获方案才能实现这一过程的良性循环和周期的缩短。这也是维护整个网络安全必不可少的环节。一旦发现异常现象，及时与反病毒公司联系。

➢ 版本升级更新管理

彻底解决新病毒的办法是保证杀毒软件的不断升级更新。为此，网络管理员应充分利用瑞星公司提供的各种升级方式，结合自身具体情况，制定合理的升级管理办法，并组织实施。

➢ 与瑞星公司的信息交流

与瑞星公司的信息交流是保证病毒防护体系不断完善的最佳途径。

2.4 瑞星杀毒软件中小企业版的特点

■国际领先的杀毒技术

瑞星杀毒软件采用了瑞星新一代病毒扫描引擎技术，继承并发扬瑞星十年的反病毒经验，可全面处理各种 DOS 病毒、Windows 3.X 病毒、Windows 9.X 病毒、宏病毒、互联网病毒、黑客程序。

■远程化管理

- ❖ 远程杀毒：网络管理员只需通过一台计算机，就可以对全网的所有计算机同时进行病毒检测和清除。
- ❖ 远程报警：局域网中任何一台计算机上发现病毒时，瑞星杀毒软件自动将病毒信息传递给网络管理员。
- ❖ 远程操作：网络管理员只需通过一台计算机，就可以对全网所有瑞星杀毒软件进行统一或个性化设置。

■自动化管理

- ❖ 自动安装：整个局域网只需在一台计算机上安装瑞星杀毒软件，即可实现对所有计算机的自动安装。
- ❖ 自动升级：系统自动从瑞星网站下载最新升级版本，并自动分发到各节点计算机，实现全网统一升级。

■功能强大，操作简便

针对以往网络版杀毒软件设置复杂，操作繁琐的弊病，瑞星采用智能化的底层优化技术，在保持功能强大的前提下，实现了界面简洁、操作便利的目标，最大限度地减少了用户操作难度和工作量。

■集中式管理、分布式杀毒

❖中央系统中心结合移动管理控制台实现全网方便管理

局域网内任意一台计算机均可设置为移动管理控制台。网络管理员通过帐号和口令使用移动管理控制台，即可清楚地掌握整个网络环境中各个节点的病毒监测状态，对局域网进行远程集中式安全管理。

❖先进的分布式管理技术

瑞星杀毒软件采用先进的分布式管理技术，调用每个节点各自的杀毒软件对该计算机上所有文件进行全面查杀病毒，解决了以往网络版杀毒软件只能查杀共享文件的缺陷。由于不在网络上传输文件，既保障了每个节点使用者的隐私，又大大提高了全网查杀病毒的效率。

■完备的服务与技术支持

瑞星公司拥有完备的病毒跟踪系统，能够及时发现各种流行和新生病毒并提供解决方案。同时，通过互联网站提供 24 小时不间断升级服务。网络管理员可自行设置升级方式，通过瑞星杀毒软件中小企业版与网络的无缝连接，以及瑞星公司自行开发的断点续传技术，使得升级既迅速及时，又安全可靠。

瑞星技术服务部为用户提供全天候技术咨询和支持，并利用遍布全国各地的服务网开展救助服务，满足用户各种需求。

第三章 安装与卸载

3.1 安装

瑞星杀毒软件中小企业版是由四个相互关联的子系统组成。安装对象包括“系统中心的安装”、“服务器端的安装”、“客户端的安装”和“管理控制台的安装”。安装首先是在服务器上安装“系统中心”，然后才能进行其他三个模块的安装。

🕮 **对服务器系统资源的要求：**

- Intel 奔腾 500MHz或更快的处理器
- 工作站32MB以上内存，服务器64MB以上内存
- 显卡：标准VGA，256色显示模式以上
- 50MB以上硬盘可用空间

🕮 **对操作系统的支持：**

- Windows NT Server 4.0
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 95/98/me
- Windows NT Workstation 4.0
- Windows 2000 Professional

◆ Windows XP

📖 对通信协议的要求：

◆ TCP/IP

3.1.1 系统中心的安装

系统中心简介

系统中心负责管理、协调瑞星杀毒软件所有子系统的工作；实现授权许可证的验证和使用；负责更新中小企业版中各系统版本更新及检测和清除病毒等工作。

提示:安装系统中心时，安装程序将在该服务器上同时安装一套服务器端系统和一套管理控制台系统。

建议系统中心的安装条件

A) 全天候开机：为确保正常实现系统中心所有功能，安装系统中心的计算机应该在有效工作期内保持全天候的开机状态。

B) 可方便上网：瑞星杀毒软件中小企业版具有自身更新、自动升级的功能，为保证此功能的顺利实现，系统中心所在服务器应能接入互联网。

C) 建议把系统中心安装在域控制器上。

提示：系统中心不要求一定安装在域控制器上，请用户在安装瑞星杀毒软件中小企业版时考虑现有网络中的资源分配。

系统中心的安装过程

首先确定准备安装瑞星杀毒软件中小企业版系统中心的服务器，对操作系统的需求请参看（本章附表 1）

安装步骤如下：

第一步：进入操作系统；

第二步：将瑞星杀毒软件中小企业版光盘放入本机的光驱内，启动瑞星杀毒软件中小企业版安装主界面后，选择【安装瑞星杀毒软件网络版】按钮，安装即开始（如图2）：

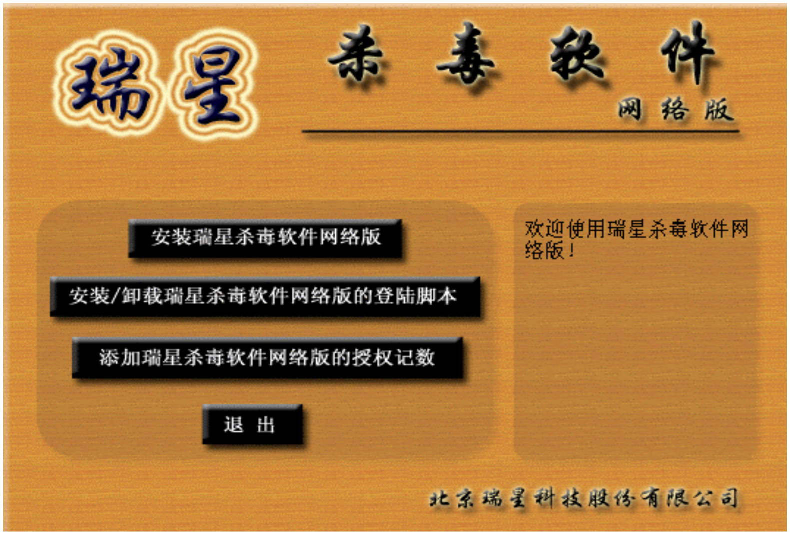


图2

提示：瑞星安装光盘内容见本章附表2。

第三步：选择【安装瑞星杀毒软件网络版】按钮后，出现瑞星安装程序引导界面（如图3），稍候进入安装界面。



图3

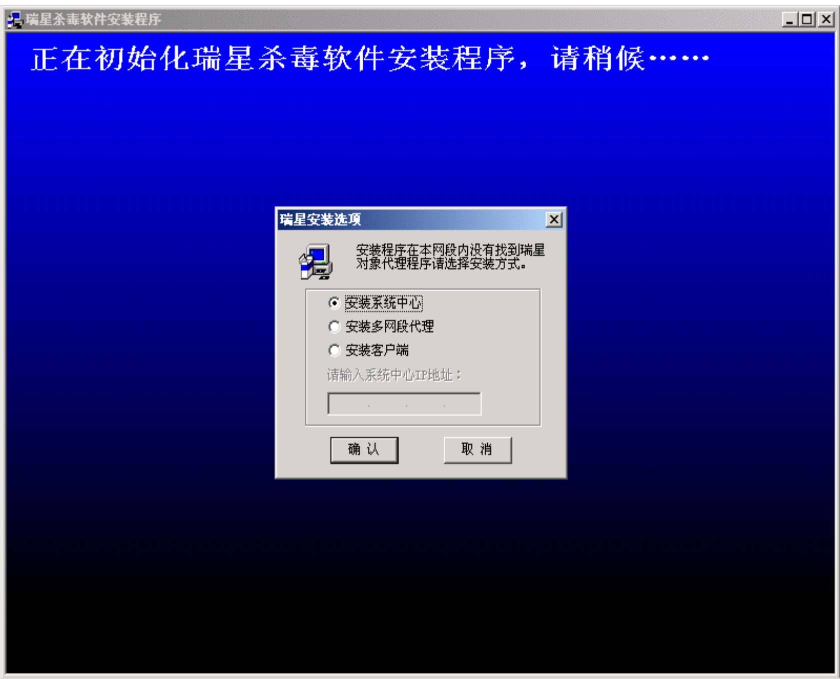


图4

第四步：安装界面出现后，选择【安装系统中心】,【确定】后继续安装（如图4）;

第五步：选择【下一步】继续安装（如图5）;



图5

第六步：出现如图6界面后，请仔细阅读『瑞星杀毒软件网络版最终用户许可协议』。如果接受，请单击【我接受】选项或者请按快捷键‘A’，然后选择【下一步】继续安装。如果不接受该协议，则单击【我不接受】选项，然后选择【取消】退出安装。

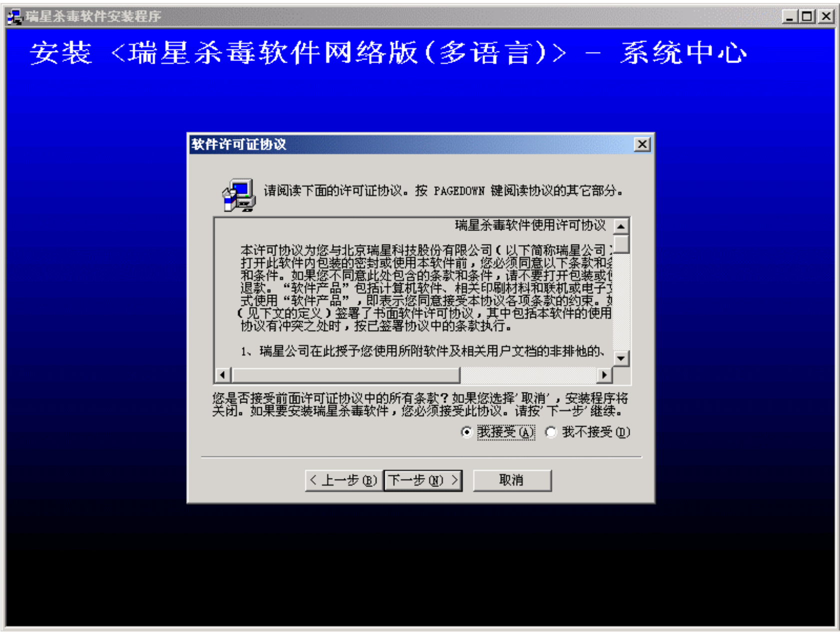


图6

第七步：输入姓名、公司名称及瑞星杀毒软件网络版产品序列号；（如图7）



图7

提示：正确输入产品序列号后，立即显示服务器和客户端允许安装的数量，如上图方框内显示。

第八步：选择【下一步】依次确认『目标文件夹』和『程序文件夹』；（如图8、图9）

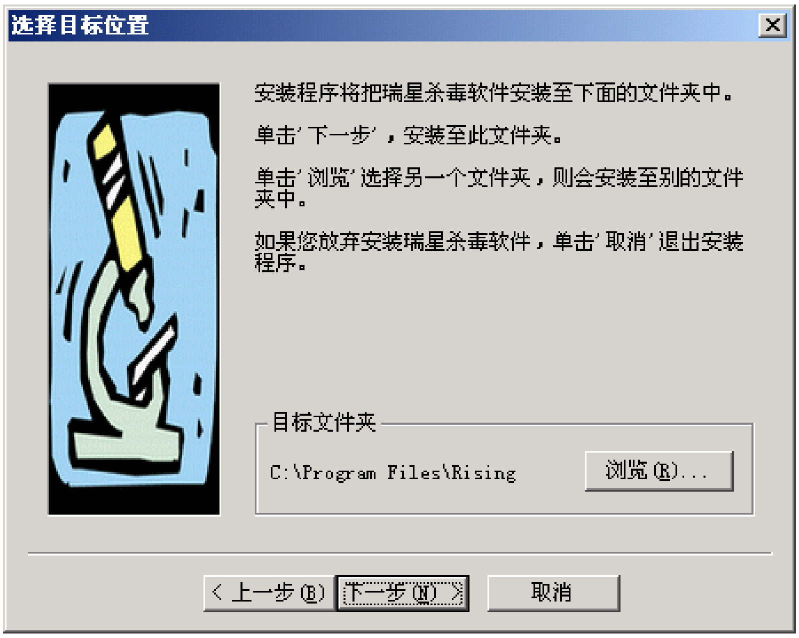


图8



图9

第九步：选择【下一步】，开始复制文件；（如图10）

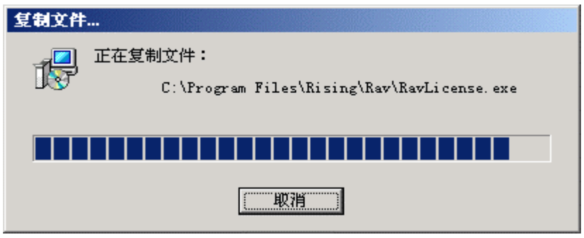


图10

第十步：文件复制结束后，系统提示是否启动管理员管理控制台和实时监控。确认后选择 【完成】结束安装；（如图11）



图11

系统中心安装结束后，弹出【管理员登录】界面（如图12），管理控制台打开。（管理控制台具体功能请参看第六章）

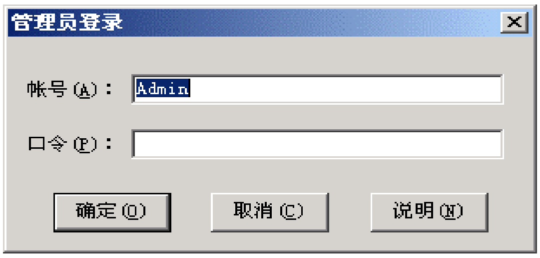


图12

提示：瑞星安装程序引导时会自动收集系统信息，如果系统中有多个IP地址，会出现下图提示（如图13）以选择瑞星系统中心所要绑定的IP地址。



图13

3.1.2 服务器端和客户端的安装

服务器和客户端采用的安装方式包含脚本安装、远程安装和本地安装，各个操作系统支持的安装方式详情参阅本章末的附表 3。

◆ 脚本安装

瑞星杀毒软件网络版利用域的启动服务概念，在域服务器上配置登录脚本。当用户登录到系统中心所在域时，实现自动为其安装瑞星杀毒软件网络版。

A)在域服务器上的脚本安装

第一步：将瑞星杀毒软件网络版光盘放入本机的光驱内，启动瑞星杀毒软件网络版安装主界面后，选择【安装/卸载瑞星杀毒软件网络版登陆脚本】按钮，安装程序即开始

第二步：程序自动检查本计算机是否为域控制器，如果计算机是域控制器则出现（如图 14）所示的安装向导界面；否则程序提示“此计算机不是域控制器，不能安装瑞星登录脚本”（如图 15），程序退出。



图 14



图 15

注意：添加脚本请选【添加瑞星用户】，卸载脚本请选【删除瑞星用户】；添加脚本和卸载脚本的以下步骤相同。

第三步：在用户列表框中选择要安装或卸载脚本的用户 （如图16）



图 16

第四步：选择【下一步】，提示是否为所选用户安装瑞星登陆脚本。选择【是】，开始安装瑞星登录脚本程序；（如图 17）

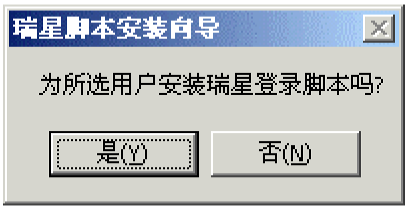


图 17

第五步：出现如图 18 所示的界面后脚本安装完成。



图 18

B)在客户端的设置，以配合脚本方式安装。

脚本登录安装是实现瑞星杀毒软件中小企业版快速自动安装的一种方法。

第一步：进入【Microsoft 网络用户】属性，选择登录到域；（如图 19）

注意：下图以 win98 为例，其他瑞星杀毒软件中小企业版支持的操作系统的具体设置请参考相关操作系统使用手册；

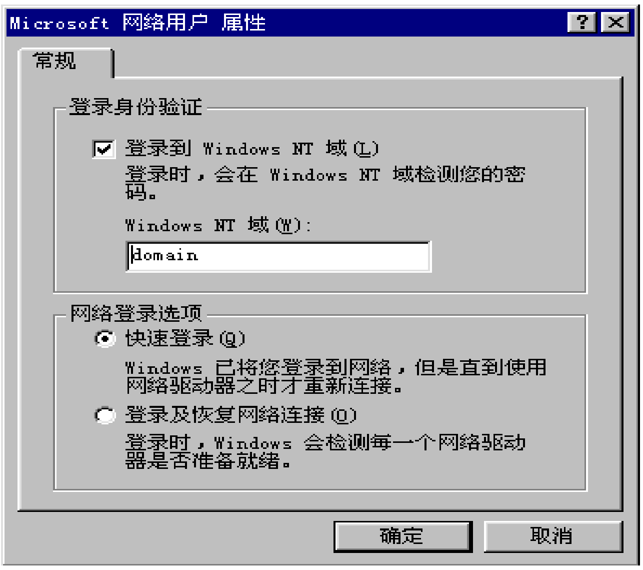


图 19

第二步：重起计算机、登录到域中，瑞星杀毒软件中小企业版的安装脚本自动运行(如图 20）。



图 20

提示：脚本登陆安装需要该计算机使用人员的参与以完成所有的安装步骤。详细情况请参看 3.1.2 节中的本地安装。

◆ 远程安装

远程安装是实现瑞星杀毒软件中小企业版快速自动安装的另一种重要方法。主要操作是在瑞星中小企业版管理控制台上完成；（详细操作请参阅 6.4.3【远程安装】）

注意：远程安装功能对操作系统的要求请参看（本章附表 3）

◆ 本地安装

本地安装是直接利用安装程序在本地完成安装的方法。无论是客户端和服务器端都可以采取本地安装的方式。

安装步骤如下：

第一步：运行光盘中的 autorun，选择【安装瑞星杀毒软件网络版】或运行光盘中的 ravsetup.exe 安装程序（ravsetup.exe 安装程序可脱离原有媒质拷贝到本地计算机中运行）

第二步：选择【安装瑞星杀毒软件网络版】按钮后，出现瑞星安装程序引导界面（如图21），稍候

进入安装界面；



图21

第三步：出现如图22和图23所示的安装界面后，程序将自动检测本机的操作系统，根据附表1的规则提示安装瑞星程序，单击【确定】后继续安装。



图22



图 23

第四步：出现如图24的界面后，请仔细阅读『瑞星杀毒软件网络版最终用户许可协议』。如果接受，请单击【我接受】选项，选择【下一步】继续安装。如不接受该协议，单击【取消】退出安装程序。

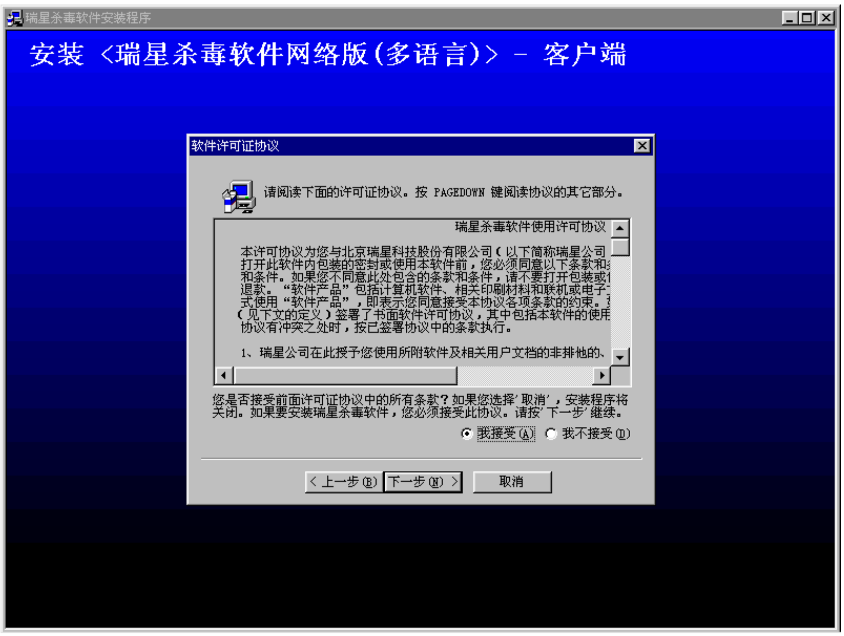


图 24

第五步：出现如图25的界面后选择安装客户端或者服务器端，单击【下一步】继续安装；



图25

第六步：选择【下一步】依次确认【目标文件夹】和【程序文件夹】；（如图26和图27）

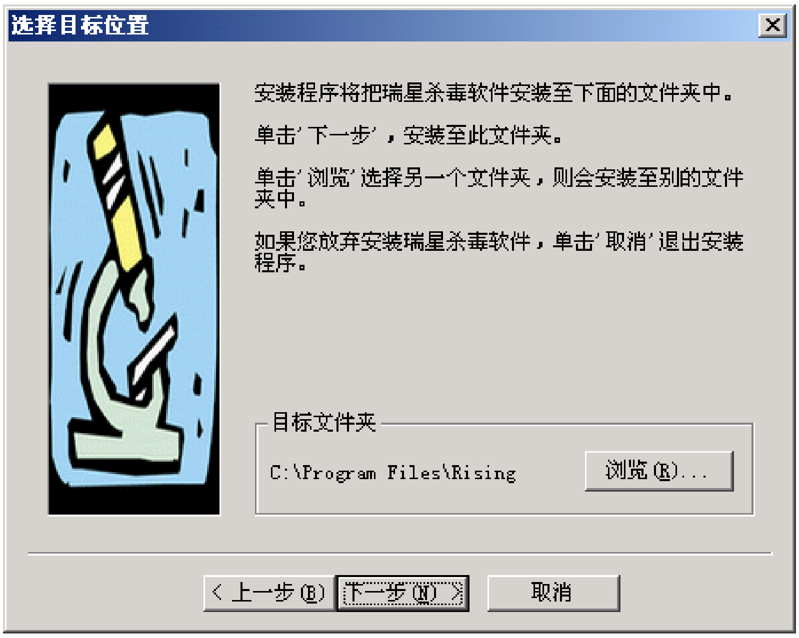


图26



图27

第七步：选择【下一步】，开始复制文件；（如图28）

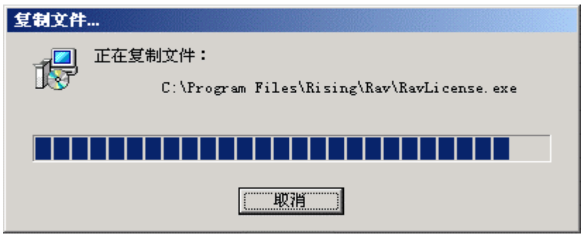


图28

第八步：文件复制结束后，提示是否启动瑞星杀毒主程序和实时监控，确认后选择【完成】结束安装；（如图29）

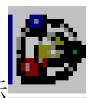


图29

提示：瑞星安装程序引导时会自动收集系统信息，如果系统中有多个IP地址，会出现下图提示选择瑞星系统所要绑定的IP地址。请您从IP列表中选择合适的IP地址。（如图30）



图30

注意：跨网段安装情况，与同网段安装不同之处是第四步，在没有安装系统中心的网段中需要安装多网段代理 。如图 31，瑞星程序会自动识别需要安装多网段代理程序的计算机。安装完毕后，多网段代理同其他瑞星程序一样驻留在后台运行,并在 windows 操作系统的状态栏中显示图标，

在双击图标弹出的窗体（如图 32）上显示系统中心的 IP 地址,并可重新指向系统中心的 IP 地址。多网段代理起到跨网段通信作用。



图 31



图 32

3.2 产品扩容

当需要增加瑞星杀毒软件中小企业版的服务器或客户端数量时，可以向瑞星公司购买一定数量的授权许可（即，扩容序列号）进行产品扩容。

注意：一套瑞星杀毒软件中小企业版所支持的客户端和服务器端总数不超过 200 个。当扩容后的序列号包含的客户端和服务器端的总数超过 200 个时，瑞星中小版程序会禁止第 201 个客户端或服务器端注册到中小企业版的防毒系统中。

扩容安装可以在局域网上任何一台安装瑞星中小企业版软件的客户端上进行。具体步骤如下：
第一步：启动瑞星杀毒软件网络版安装主界面的【添加瑞星杀毒软件网络版的授权计数】（运行光盘上的 Ravsetup.exe 也可以实现相同的功能），如图 33。

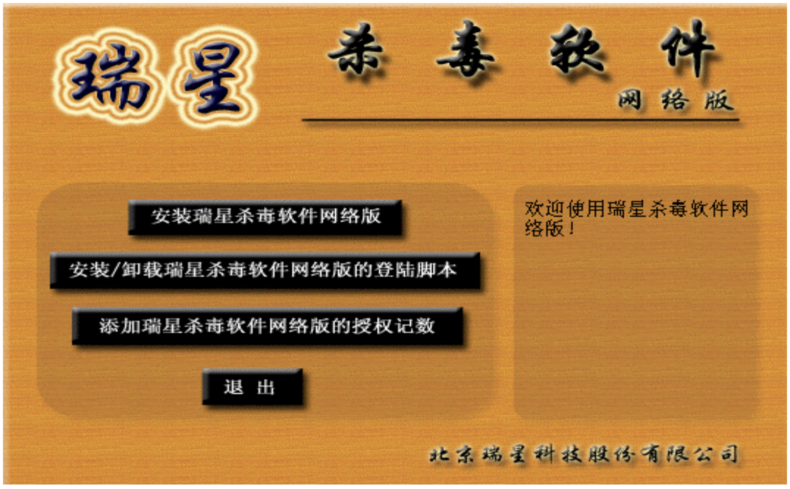


图 33

第二步：确认『许可协议』（如图 34），按【下一步】继续；

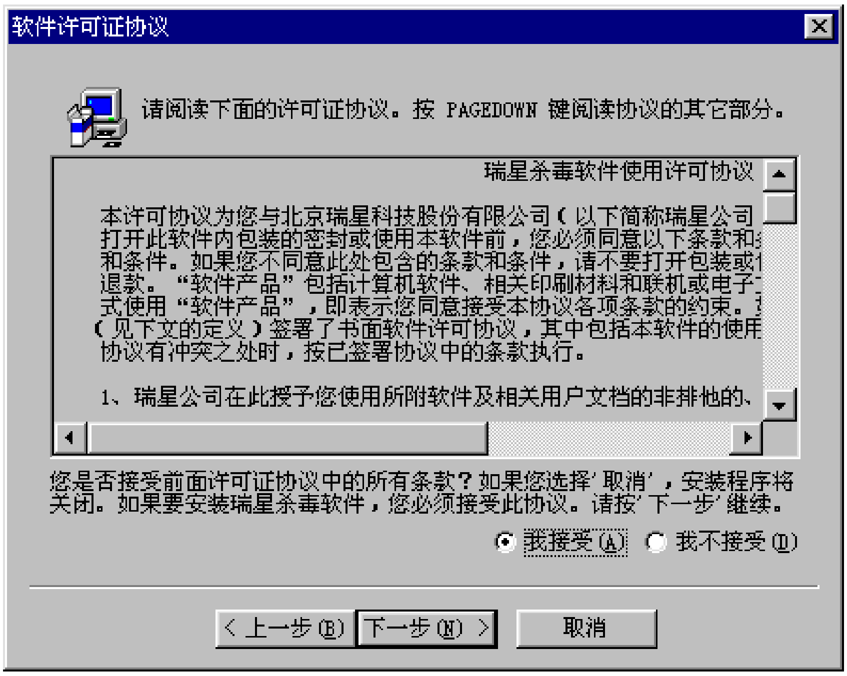


图 34

第三步：选择【添加 License 计数】，按【下一步】继续（如图 35）；



图 35

第四步：输入瑞星公司提供的扩容序列号，添加同时显示本次添加的服务器端和客户端数量；（如图 36）

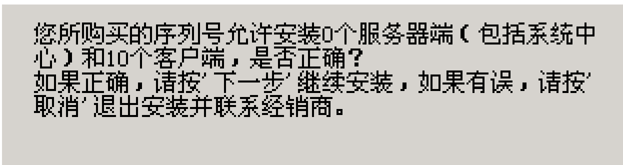


图 36

第五步：按【下一步】，显示当前总授权记数（如图 37），按【确定】完成添加；



图 37

3.3 卸载

瑞星杀毒软件中小企业版提供了全自动的卸载功能。卸载有两种方式：利用瑞星卸载程序卸载和利用控制面板的【添加/删除程序】卸载。

3.3.1 利用瑞星软件卸载程序

第一步：依次进入【开始】/【程序】/【瑞星杀毒】，选择【卸载瑞星软件】；（如图 38）



图 38

第二步：确定后进行软件的卸载。（如图 39）

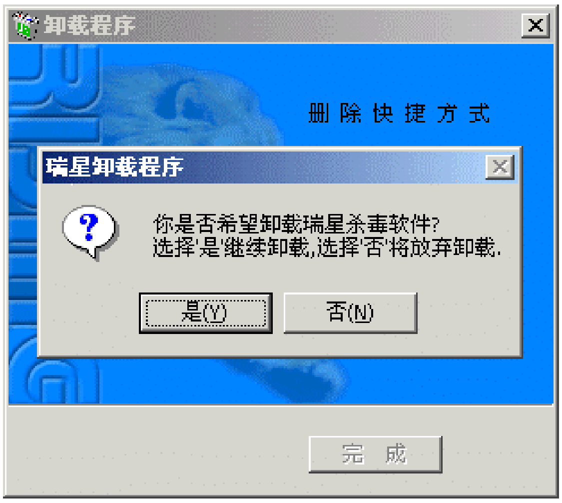


图 39

第三步：卸载完毕出现提示界面（如图 40）。



图 40

3.3.2 利用控制面板的【添加/删除程序】卸载

第一步：打开控制面板，双击【添加/删除程序】；（如图 41）



图 41

第二步：在【安装/卸载】属性页中选中 【瑞星杀毒软件】，然后按【添加/删除】按钮，自动卸载，卸载过程同 3.3.1 节。

附表 1：

系统中心、服务器端和客户端在安装时所需操作系统

	系统中心	服务器端	客户端
Win95			√
Win98			√
WinMe			√
WinNt WorkStation			√
WinNt Server	√	√	
Win2000 professional			√
Win2000 Server	√	√	
Win2000 Advanced Server	√	√	

附表 2：

瑞星安装光盘内容

序号	文件名	功能介绍
1	RavSetup.exe	瑞星杀毒软件中小企业版安装程序
2	Ravscript.exe	登录脚本安装程序
3	Autorun.exe	瑞星杀毒软件中小企业版安装主界面
4	Autorun.inf	光盘自启动配置文件
5	RavCheck.exe	瑞星杀毒软件中小企业版辅助安装程序

附表 3：

本地安装、脚本安装和远程安装所需的操作系统

		本地安装	脚本安装	远程安装
客户端	Win95	√	√	
	Win98	√	√	
	WinMe	√	√	
	WinNt WorkStation	√	√	√
	Win2000 professional	√	√	√
服务器端	WinNt server	√	√	√
	Win2000 server	√	√	√

第四章：客户端本地杀毒

瑞星杀毒软件不仅可以通过系统中心进行全网和定制的查杀毒，也可以启动在本地的瑞星杀毒软件杀毒，以实现多方式多角度的防毒，确保病毒无“藏身之地”。

4.1 本地杀毒软件的启动

方法一：可以双击桌面的【瑞星杀毒软件】图标启动瑞星本地的杀毒软件。

方法二：可以点击开始菜单中的【瑞星杀毒软件】程序组来启动瑞星杀毒软件。（如图 42）

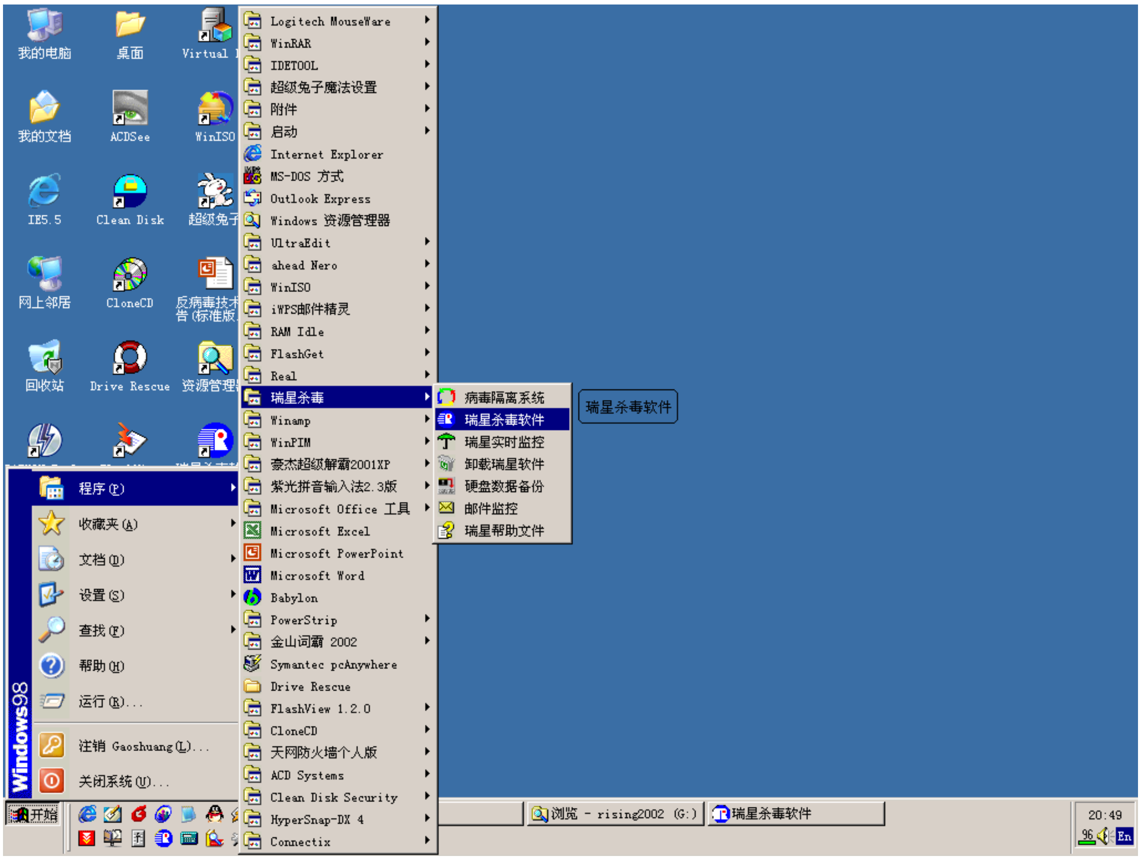


图 42

方法三：可以双击系统托盘区的瑞星实时监控图标或者右键点击图标，在弹出的菜单处选择【启动瑞星杀毒软件】就可以启动瑞星主程序。

启动瑞星主程序，随即弹出杀毒主界面。（如图 43）



图 43

4.2 杀毒软件应用与设置

通过瑞星杀毒软件菜单选项的设置可以确定杀毒的目标，文件类型等个性化的杀毒设置。可以确定更明确的杀毒目标和病毒处理方式。

4.2.1 界面按钮的应用

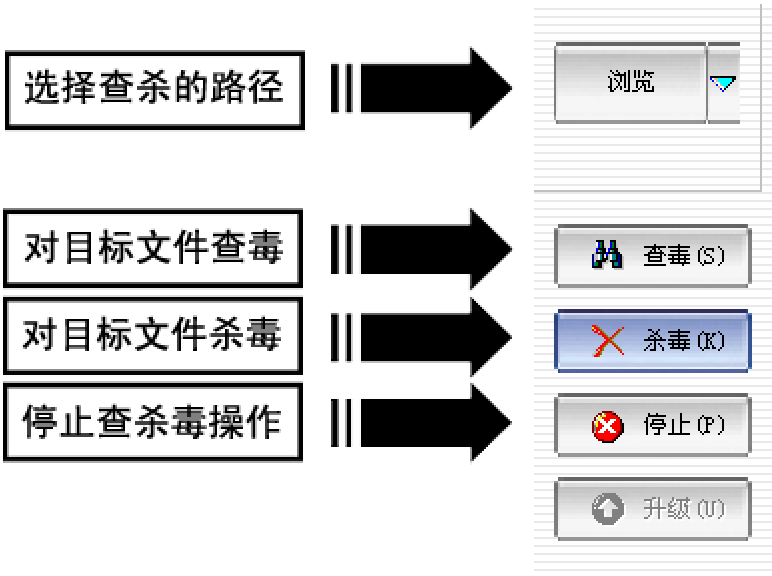


图 44

4.2.2 菜单的应用与设置

杀毒主界面有【操作】、【设置】、【工具】和【帮助】等几个菜单项（如图 45)。用户可以通过菜单项所提供的功能选项完成自己个性化的杀毒计划和杀毒设置，备份数据和了解病毒信息等工作。



图 45

◆ 【操作】菜单的应用

单击菜单【操作】或者在瑞星杀毒主程序下点击键盘（O）可以打开杀毒软件的操作菜单。操作菜单的功能如下（见图 46)。

A)【操作】菜单项：

此菜单项中的【查毒】、【杀毒】和【停止】的功能与 4.2.1 中对应按钮的作用完全相同。



图 46

B)【历史记录】项：

1、 单击菜单中的【历史记录】或单击键盘（R）键弹出杀毒的病毒信息。(如图 47)



图 47

2、 您可以通过下拉框的选项选择不同条件下处理的病毒信息。

3、 单击【清空】按钮可以删除相对应条件下的病毒信息。

4、 单击【导出】按钮可以将历史记录生成一个.txt 文本报告。（如图 48）

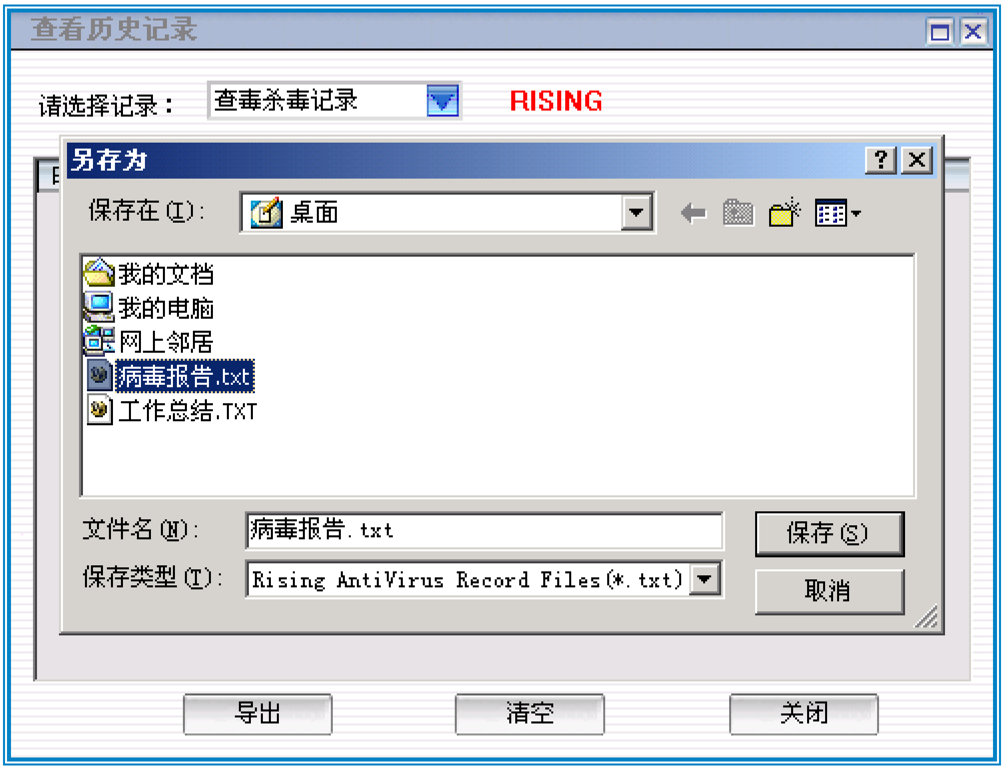


图 48

C）【显示信息列表】项：

单击对应菜单选项或点击键盘（M）键可以得到相关的操作错误信息。

D）【退出】项：

单击对应菜单选项或者点击键盘（X）键可以退出瑞星杀毒主程序。

◆ 【设置】菜单的应用

单击菜单【设置】或者在瑞星杀毒主程序下点击键盘（C）可以打开杀毒软件的设置菜单，对应的功能项（如图 49）。

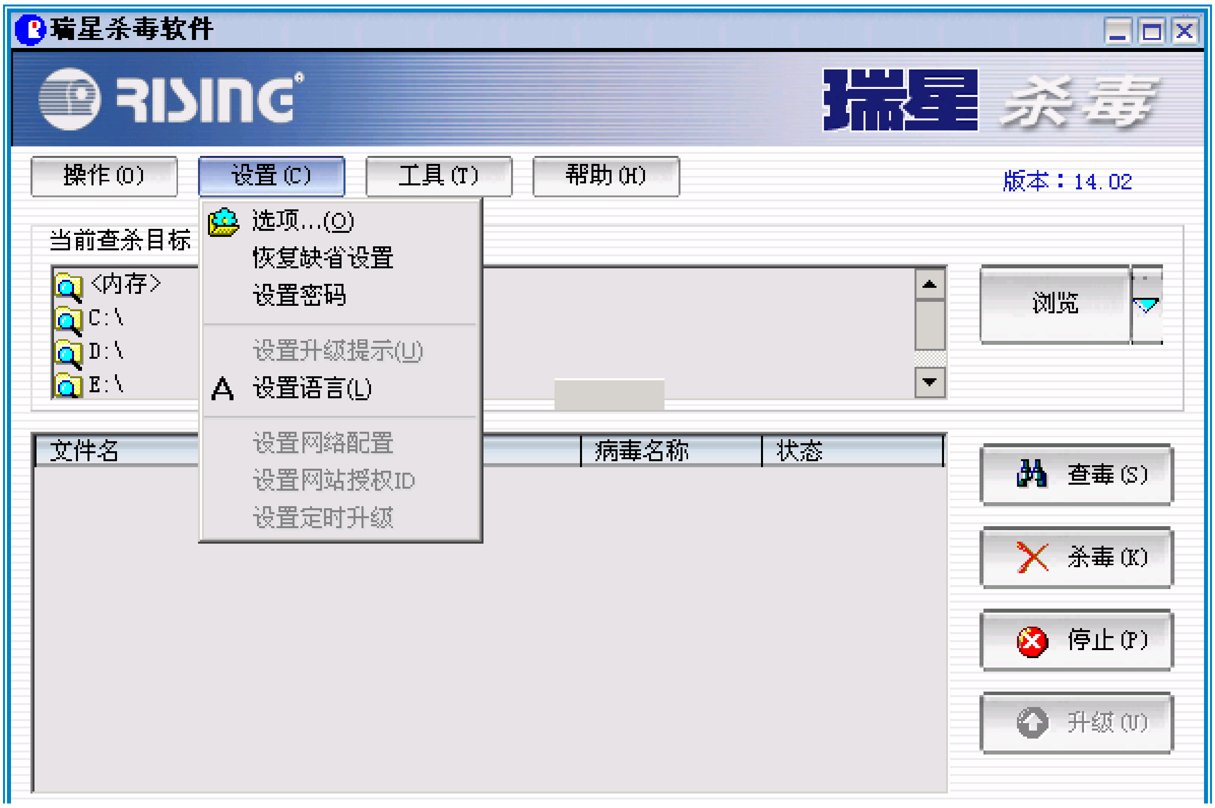


图 49

A）【选项】菜单项：

【设置】菜单中的【选项】是瑞星杀毒软件体现个性化操作设置的核心部分。用户可以通过对其中不同参数的设置来制定自己的查杀毒计划和处理方式。

1、【查杀设置】项：

点击【选项】后到默认的【查杀设置】的界面（如图 50）

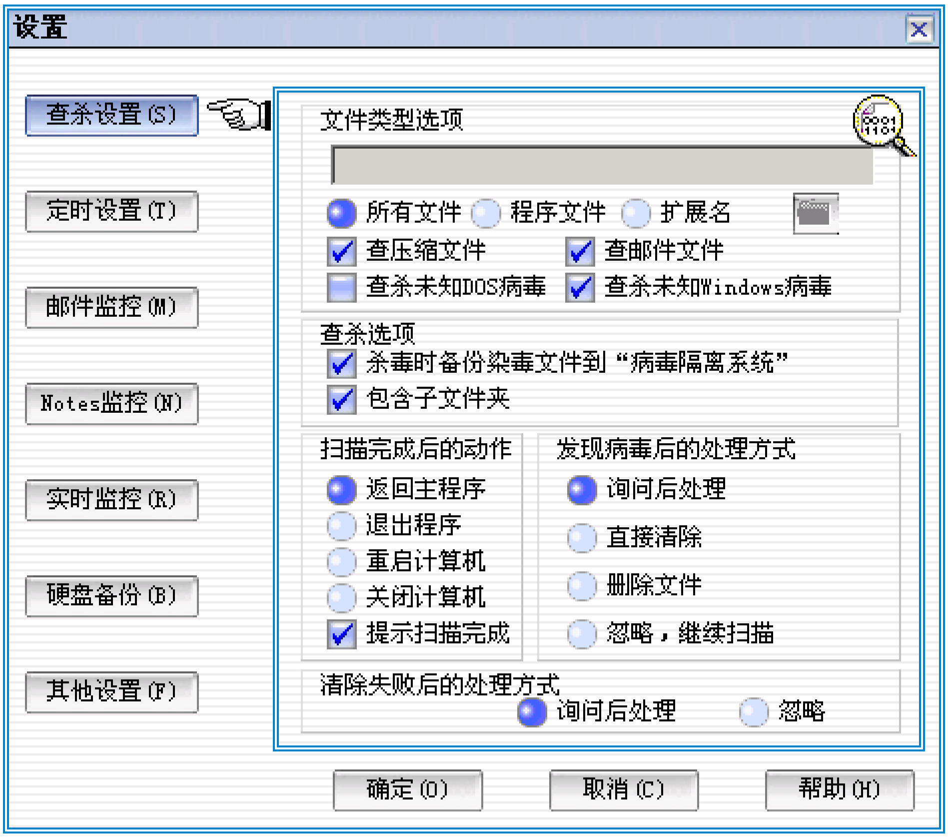


图 50

（1）文件类型选项

您可以通过对文件类型的选择确定要查杀的目标文件的类型。

【所有文件】项：选择后将监测任何格式的文件。

【程序文件】项：选择后将监测EXE、COM、SYS、VXD、DRV、DLL、BIN、OVL、386、SRC、HTM、HTML、FON、VBS、DOC、DOT、XLS、XLT等扩展名的文件。

【扩展名】项：选择后可以在提供的输入栏中输入需要的文件类型的扩展名，或者点击按钮在弹出的对话框中（如图51）根据自己的需要进行相应的文件类型的选择。

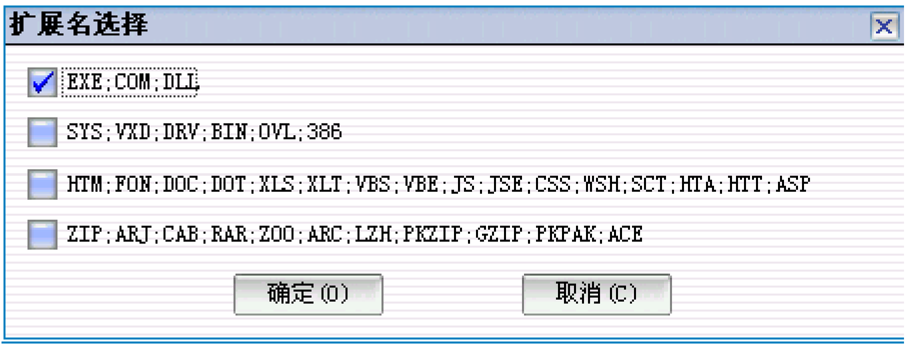


图51

【查压缩文件】：此选项被选中将查杀ZIP、ARJ、CAB、ZOO、RAR、ARC、LZH、GZIP等扩展名的压缩或自解压文件。

【查邮件文件】：选择后可以查杀所有识别的邮箱和邮件文件。

【查杀DOS病毒】：此选项被选中后可检测出携带未知的DOS病毒，您可以直接进行查杀处理或把可以的文件发给瑞星公司进行分析。

【查未知Windows病毒】：此选项被选择后可检测出携带未知Windows病毒的文件，包括未知宏病毒和脚本病毒等。

（2）查杀选项

【杀毒时备份染毒文件到“病毒隔离系统”】：此项选中后,将会把所有您清除或删除的染毒文件备份在【病毒隔离系统】中隔离起来，如果您认为备份到病毒隔离系统中的染毒文件还有其它用途，可以从病毒隔离系统中将其恢复。（详细应用方法请见“4.3.1 病毒隔离系统”节。）

【包含子文件夹】：此选项被选择后将检测子文件夹中的文件是否带有病毒；如果不选，将只查杀指定的当前目录。

（3）扫描完成后的动作

【返回主程序】：此选项被选择后，查毒完成后将自动返回到瑞星主程序。

【退出程序】：此选项被选择后，查毒完成后将自动退出瑞星主程序。

【重启计算机】：此选项被选择后，查毒完成后将自动重新启动计算机。

【关闭计算机】：此选项被选择后，查毒完成后将自动关闭计算机。

【提示扫描完成】：为了方便查看和明确查杀结果，您选中该选项后，当扫描完成时会出现本次查杀病毒具体信息的提示。（建议用户选择 【提示扫描完成】的方式）

（4）发现病毒后的处理方式

【询问后处理】：此选项被选择后，查毒过程中发现病毒将询问用户如何处理。（建议用户使用“询问后处理）的方式）。

【直接清除】：此选项被选择后，查毒过程中发现病毒后将直接清除而不提示任何信息。

【删除文件】：此选项被选择后，查毒过程中发现病毒后将直接删除带毒文件。

【忽略，继续扫描】：此选项被选择后，查毒过程中发现病毒将不作任何处理继续进行扫描。

（5）清除失败后的处理方式

清除失败后可选择 【询问后处理】和【忽略】两种方式，进一步保证即不漏过也不错杀可疑文件。

以上设置结束后，点击【确定】按钮，即可生效。如需返回缺省设置，请选择【设置】菜单中的「恢复缺省设置」命令即可。

2、菜单【定时设置】项 ：

点击【选项】进入【定时设置】的界面（如图 52）

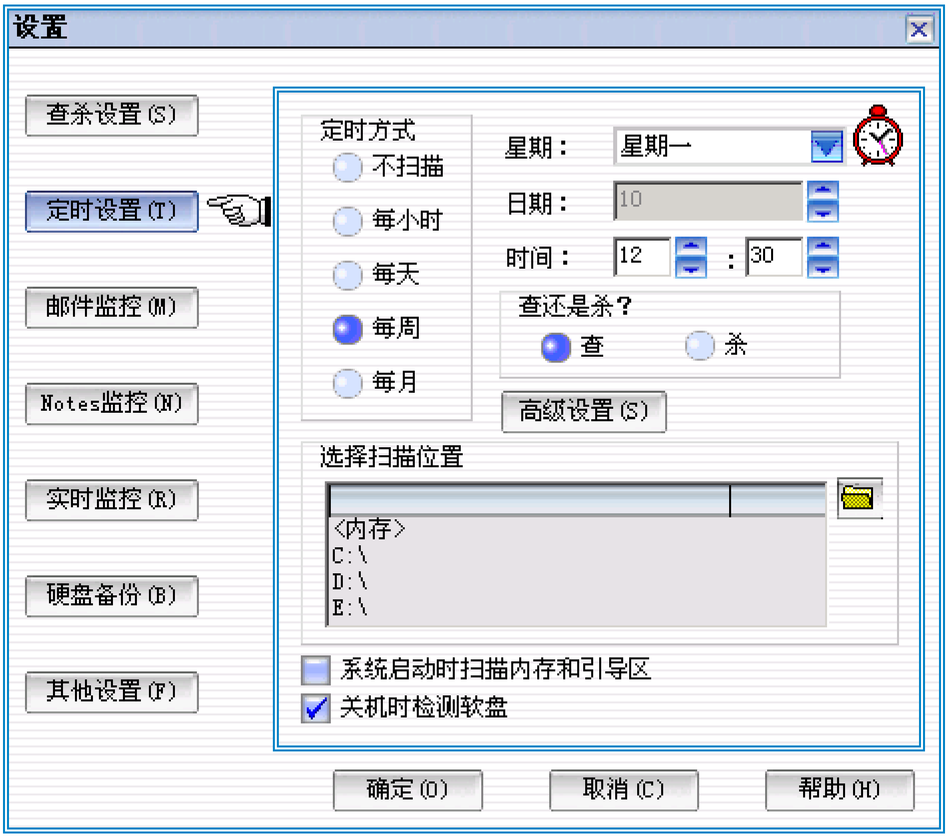


图 52

（1）定时方式：

时间定时设置方式：

根据不同的需要，不同的用户可以在定时查杀病毒设置页面选定自己希望瑞星杀毒软件【网络版】对自己的计算机进行定时查杀的时间，可在时间设置内分别选择【不扫描】、【每小时】、【每日】、【每周】、【每月】等不同扫描频率；（如每小时或每日 10：00 或每周，星期一，12：00 或每月，10 日，10：00）。

【高级设置】：

您还可以根据自己对计算机掌握程度的不同来决定是否进入【定时查杀高级设置】选项来进一步详细的设置您的定时查杀功能。（高级设置方法可参照 【查杀设置】里的方式。）

（2）选择扫描位置：

在【选择扫描位置】中可点击  指定需要定时检测的磁盘或文件夹。（如图 53）

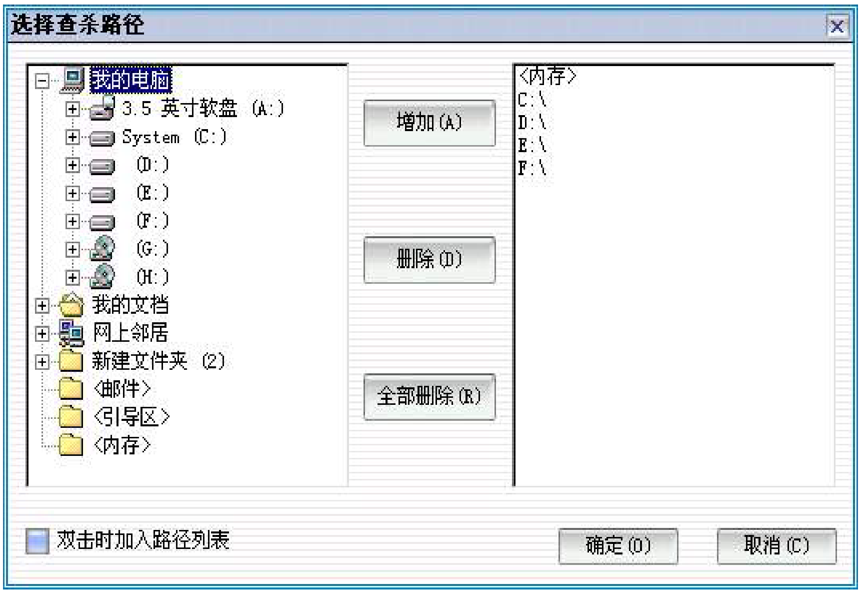


图 53

【系统启动时扫描内存和引导区】：此项功能选择后，每次系统启动进入时将会扫描内存和引导区，以保证您有干净的系统环境来开始工作。

【关机时检测软盘】 ：此项功能选择后，每次系统关闭时会检查软区里的软盘是否带毒，防止下次系统启动时感染引导型病毒。

3、【邮件监控】项：

点击【选项】、【邮件监控】，进入【邮件监控】设置界面（如图 54）

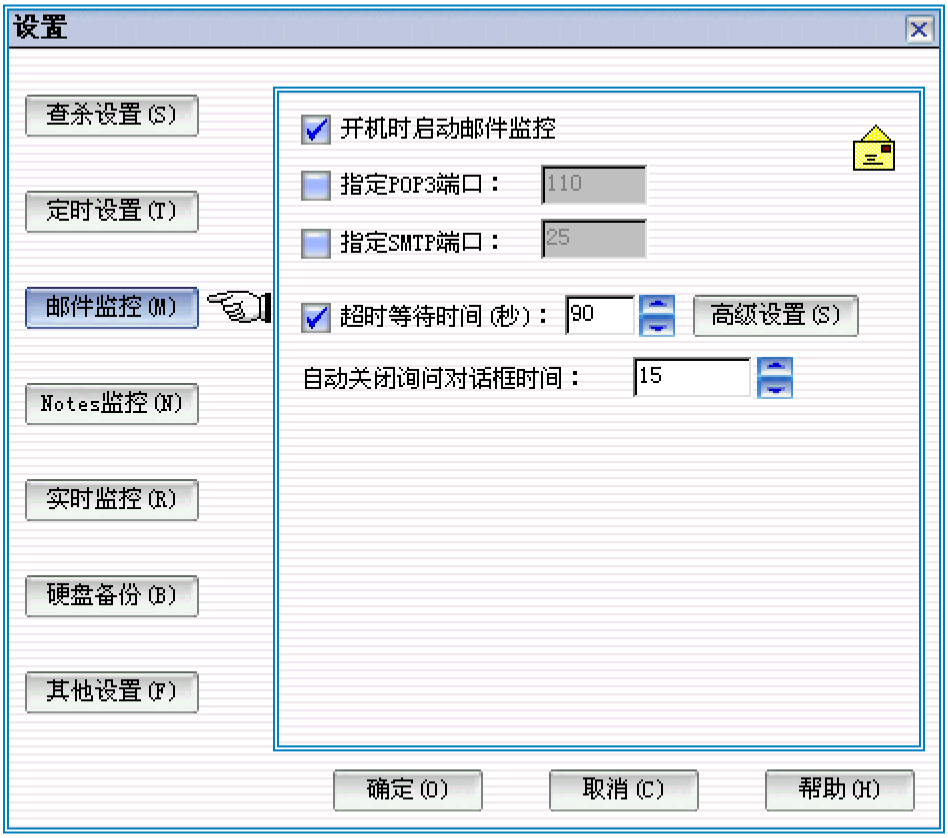


图 54

邮件监控是【瑞星杀毒软件】新增功能，当您使用 Microsoft Outlook 或 Outlook Express 等软件接收、发送和阅览电子邮件时，如果邮件附件染毒，邮件监控会立即提醒您并提供多种方式对含染毒附件进行处理。（具体使用方法和设置请参阅“5.2 邮件监控”节）

4、【Notes 监控】项：

点击【选项】、【Notes 监控】，进入【Notes 监控】界面（如图 55）

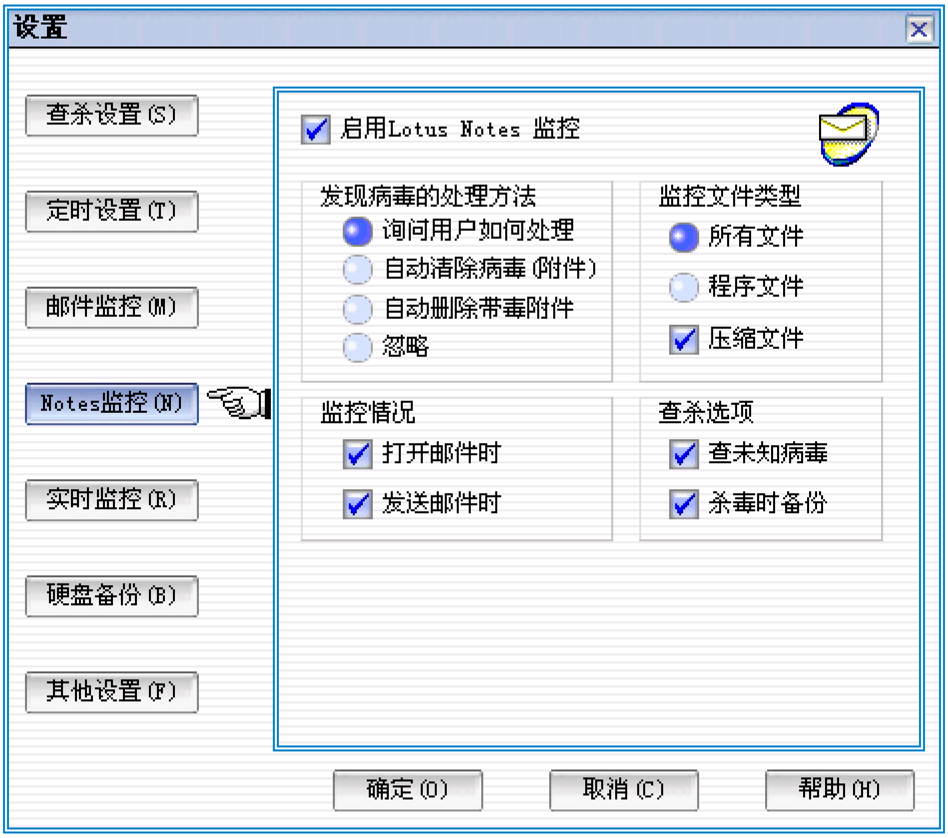


图 55

如果您安装了 Lotus Notes,可以通过【Notes 监控】对 Lotus Notes 邮件监控进行设置（使用方法和设置请参阅 5.3），Notes 邮件监控是可选组件，典型安装中会自动安装在您的机器中，您也可在安装过程中进行选择。

注：对 Lotus Notes 邮件监控设置更改后，需要重新启动 Lotus Notes 设置才能生效。

5、菜单【实时监控】项：

点击【选项】进入【实时监控】的界面（如图 56）（实时监控使用方法和设置请参阅 5.1）

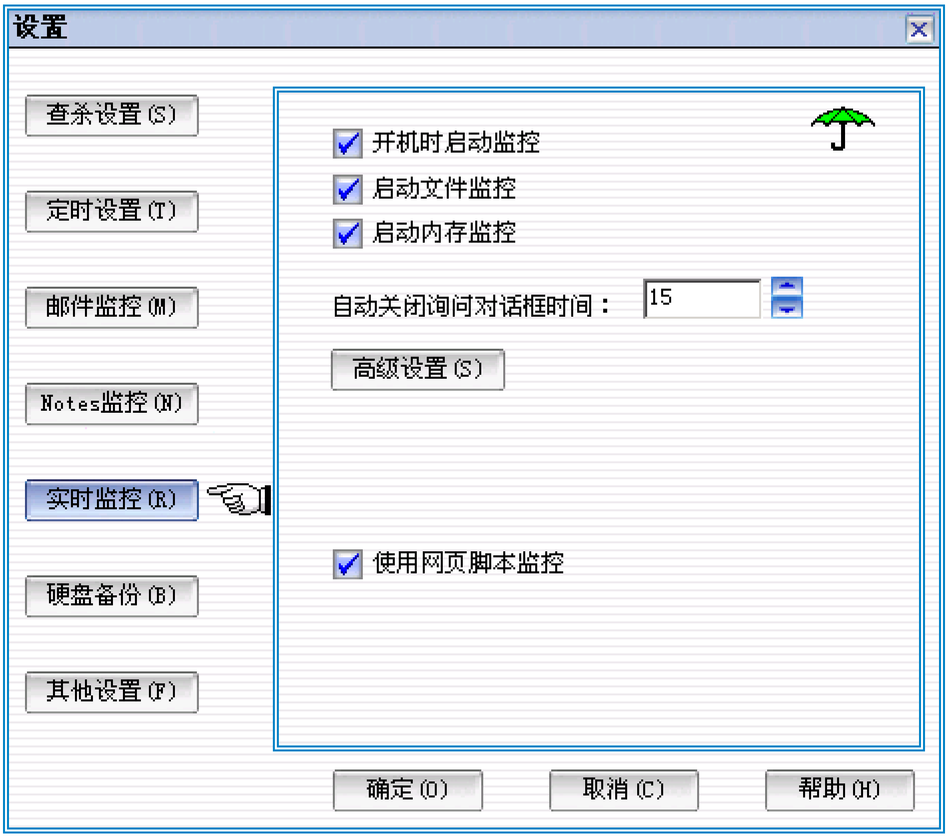


图 56

6、【其他设置】项 ：

点击【选项】进入【其他设置】的界面（如图 57）

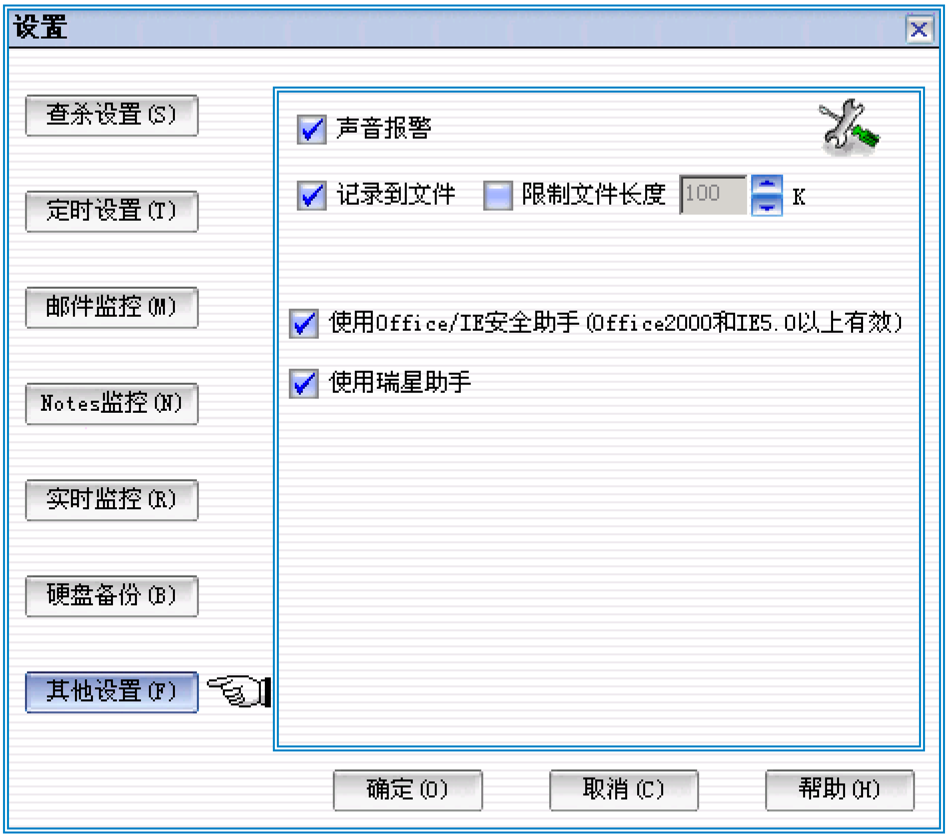


图 57

【声音报警】:此项功能选择后，在检测到病毒时，瑞星软件将通过声卡或 PC 喇叭两种方式（由电脑配置自动选择）提醒您注意。如您不需要声音报警也可以关闭。

建议：如果您希望加快查杀速度，请关闭声音报警。

【记录到文件】:此项功能选择后，您可以设置检测到病毒时是否写入历史记录，并限制历史记录文件的长度。

【使用 Office/IE 安全助手】:此项功能选择后，当您使用 Office2000 和 IE 的时候，瑞星的安全助手能提供保护功能。当该选项处未选状态时，瑞星安全助手不起作用。

注：该功能只在 Office2000 和 IE 5.0 以上时，才可以有效使用。

【使用瑞星助手】:选中该项后，每次启动瑞星程序时都会启动瑞星助手。（详细信息见 4.3.3）

7、【硬盘备份】项：

点击【选项】进入【硬盘备份】的界面（如图 58）

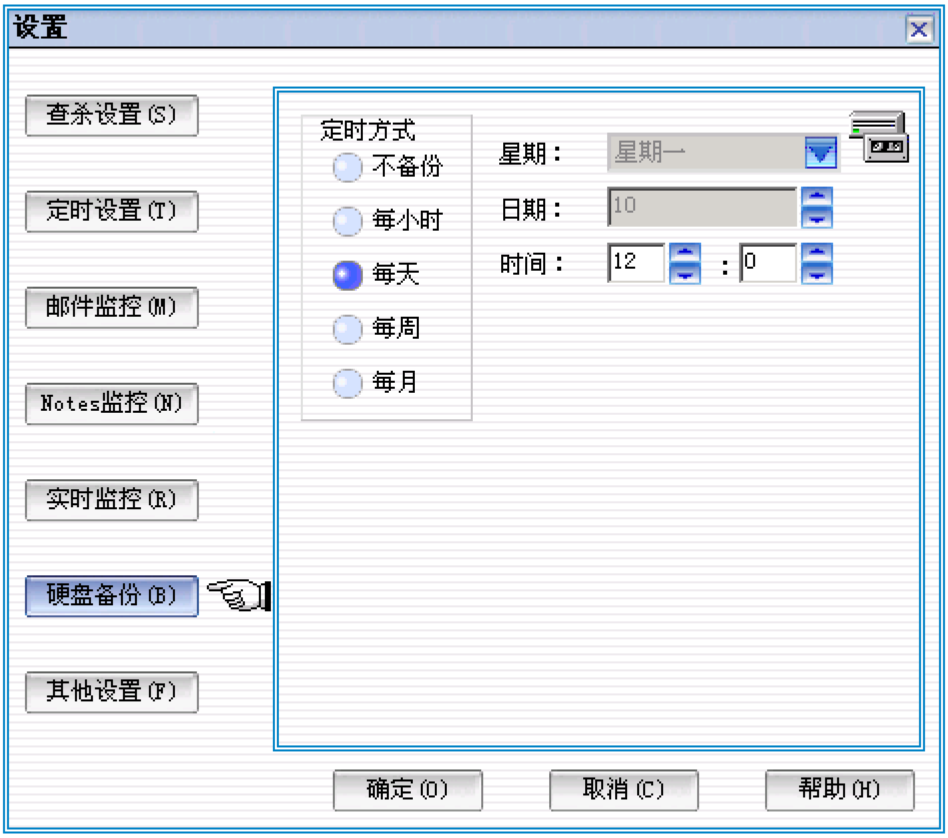


图 58

选择【备份设置】后，您可以在主程序的设置选项中，设置定时备份，以保障您的备份文件是最新的。（详细应用方法请见 “4.3.2 硬盘数据备份”节）

A）【恢复缺省设置】 菜单项：

第一次启动瑞星杀毒软件，程序的功能设置是默认的，您可以在此菜单的【设置】项中以您习惯的方式设置软件所有的功能。若您在设置完之后在使用中想恢复【默认的设置】可选择【恢复缺省设置】，将为您恢复默认的设置。（如图 59）



图 59

B）【设置密码】菜单项：

此项设置选择后，可以保护您本地的瑞星查杀设置选项内的调整不被他人修改。（如图 60）



图 60

注：第一次修改密码时，旧密码为空。

C）【设置语言】菜单项：

设置语言功能是瑞星添加的一项新功能。在此设置了多语言信息，您可以根据操作系统的语言版本来更改相应的语言设置。（如图61）

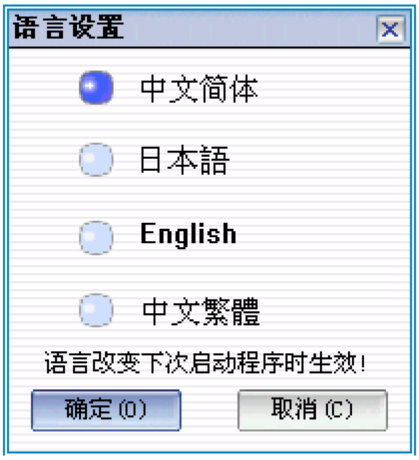


图 61

提示：该功能设置后需要重新启动瑞星程 序时才能生效。

◆ 【工具】菜单的应用

【工具】菜单中提供了一些工具和快捷功能，可以帮助您更方便的使用杀毒软件及保护数据的安全。其中包括【开/关实时监控】、【开/关邮件监控】、【病毒隔离系统】、【硬盘数据备份】和【制作安装盘】等几个菜单项（如图 62）。



图 62

A)【开/关实时监控】菜单项：

此工具在实时监控未打开时可以立即启动实时监控；若实时监控已打开，此工具将关闭实时监控，此时将不监控任何目标是否带毒。

B)【开/关邮件监控】菜单项：

此工具在邮件监控未打开时可以立即启动邮件监控；若此邮件监控已打开，此工具将关闭邮件监控，此时将不监控邮件是否带毒。

C)【病毒隔离系统】菜单项：

在安装瑞星软件的同时，病毒隔离系统将自动安装到当前计算机系统中，并在瑞星杀毒软件程序组里建立快捷方式。通过【病毒隔离系统】工具可以及时的恢复带毒文件。（详细应用方法请见【4.3.1 工具的应用】里的病毒隔离系统。）

D)【硬盘数据备份】菜单项：

在安装瑞星软件的同时，硬盘数据备份系统将自动安装到当前计算机系统中，并在瑞星杀毒软件程序组里建立快捷方式。您可以选用硬盘备份定时方式来选择不备份或者指定每小时、每天、每周、每月的任何时间开始进行数据备份。

通过定时备份可以保证您的数据备份是较新的，这样当你需要恢复数据时才能最大限度的减少损失。（设置方法详见“4.3.2 硬盘数据备份”节）

E)【制作瑞星 DOS 盘】菜单项：

此项设置可以更新瑞星产品中的两张 DOS 盘，用户可以按需制作升级。（详细升级方法请参见 7.4 章节。）

F)切换界面菜单项：

瑞星杀毒软件采用独特的多界面设计，豪华与朴实相结合，个性化的选择，给您以美的享受。此功能可以使您通过切换界面来设定个性化的瑞星杀毒软件。（如图 63、图 64、图 65 和图 66）



图 **63** 灰色天空


瑞星杀毒软件
RISING
瑞星 杀毒
操作(O)
设置(C)
工具(T)
帮助(H)
版本：14.02
当前查杀目标
<内存>
C:\
D:\
E:\
浏览
文件名
所在文件夹
病毒名称
状态
查毒(S)
杀毒(K)
停止(P)
升级(U)
北京瑞星科技股份有限公司

图 64 守望的狮子


瑞星杀毒软件
操作(O)
设置(C)
工具(T)
帮助(H)
版本：14.02
当前查杀目标
<内存>
C:\
D:\
E:\
浏览
文件名
所在文件夹
病毒名称
状态
查毒(S)
杀毒(K)
停止(P)
升级(U)
北京瑞星科技股份有限公司

图 **65** 大浪淘沙



图 66 爱尔兰咖啡

◆ 【帮助】菜单的应用

瑞星杀毒软件提供了系统详细的帮助，其中包括【帮助主题】、【日积月累】、【瑞星公司主页】和【关于瑞星】等几个菜单项（见图 67）。



图 67

A)【帮助主题】菜单项：

此项选择后，在您使用瑞星杀毒软件的过程中，遇到疑问和操作方法上的问题时，帮助主题可以为您提供的详细帮助信息。

B)【日积月累】菜单项：

若您想了解有关病毒方面的资料或有关瑞星公司的情况，请您打开【日积月累】，查看您所关心的内容，（如图 68）所示。如果您不需要每次启动瑞星杀毒软件的同时启动日积月累请把‘启动时显示’的标记去掉。

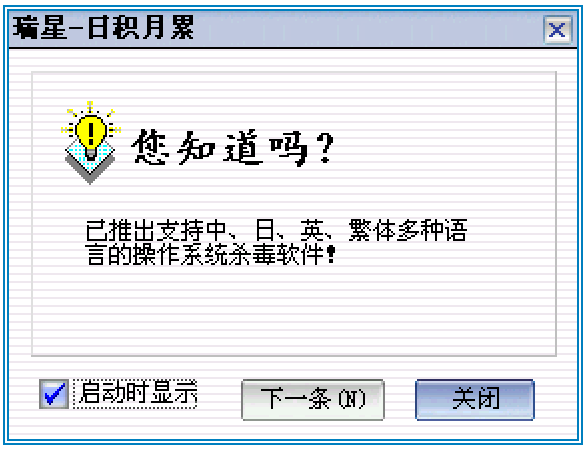


图 68

C)【瑞星公司主页】菜单项：

程序可通过此选项自动登陆浏览瑞星主页。您也可以直接在任何一个互联网浏览器中键入“www.rising.com.cn”访问瑞星公司主页。（如图 69）



图 69

D)【关于瑞星】菜单项：

在此您可查看您软件的版本号、程序更新日期以及瑞星公司的详细地址和联系方式。（如图 70）

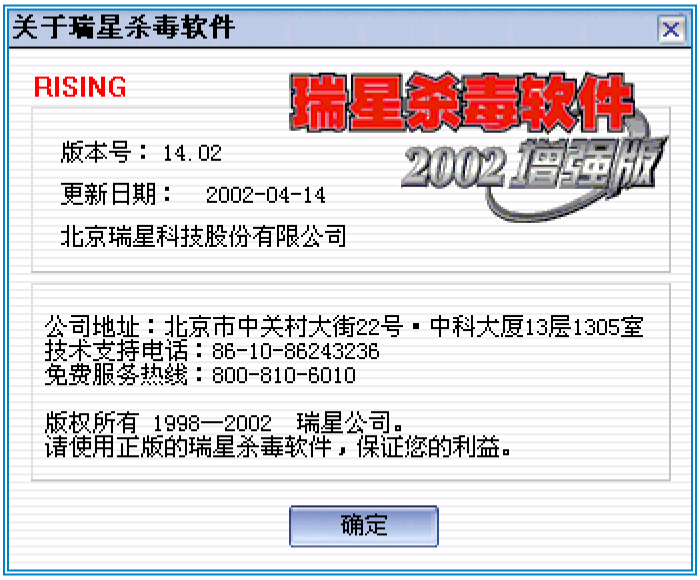


图 70

4.3 工具的应用

4.3.1 病毒隔离系统

只要您选择了【杀毒时备份染毒文件到“病毒隔离系统”】，此系统将保存染毒文件的备份。在此系统中，保存了您完整的文件备份，如果您希望恢复带毒文件，您可以在此系统中将带毒文件备份还原。完全保护您重要资料。此系统为您提供方便的图形界面操作。（如图 71）



图 71

◆ 【操作】菜单的应用：

单击菜单‘操作’或者在病毒隔离系统下点击键盘（F）可以打开病毒隔离系统的‘操作’菜单。（如图 72）



图 72

A)菜单【恢复】项：

如果您认为备份到病毒隔离系统中的染毒文件还有其它用途，此项选中后，可以从病毒隔离系统中将染毒文件恢复到清毒前文件原有的目录下。

B)菜单【恢复为】项：

如果您认为备份到病毒隔离系统中的染毒文件还有其它用途，此项选中后，可以从病毒隔离系统中将其恢复到指定的目录下。

C)菜单【删除】项：

如果您认为备份到病毒隔离系统中的染毒文件已没有其它用途，此项选中后，将从病毒隔离系统中彻底删除染毒文件。

注意：备份文件一经删除不可恢复。

D)菜单【清空】项：

如果您认为备份到病毒隔离系统中的染毒文件已没有其它用途，此项选中后，将完全清空病毒隔离系统里备份的染毒文件。

注意：备份文件一经清空不可恢复。

◆【选择】菜单的应用：

单击菜单‘选择’或者在病毒隔离系统下点击键盘（S）可以打开病毒隔离系统的‘选择’菜单。（如图 73）



图 73

此菜单可以让您选择需要的染毒文件，进行操作。

A) 菜单【全部选定】项：选此项或按键盘组合键 Ctrl+A，可以选择全部文件。

B) 菜单【反向选择】项：选中某些文件后选此项，将已选定文件标志为未选定，将未选定文件标志为已选定。

C) 菜单【相同时间保存的文件】项：选中某个文件后选择此项，将自动选定跟此文件同时保存的染毒文件。

D) 菜单【相同路径保存的文件】项：选中某个文件后选择此项，将自动选定与此文件隔离前路径相同的文件。

E) 菜单【被相同病毒感染文件】项：选中某个文件后选择此项，将自动选定与此文件感染相同病毒的文件。

◆ 【查看】菜单的应用：

单击菜单‘查看’或者在病毒隔离系统下点击键盘（V）可以打开病毒隔离系统的‘查看’菜单。（如图 74）



图 74

此菜单可以让您方便的查看所需染毒文件的信息。

◆ 【工具】菜单的应用：

单击菜单‘工具’或者在病毒隔离系统下点击键盘（T）可以打开病毒隔离系统的‘工具’菜单。（如图 75）

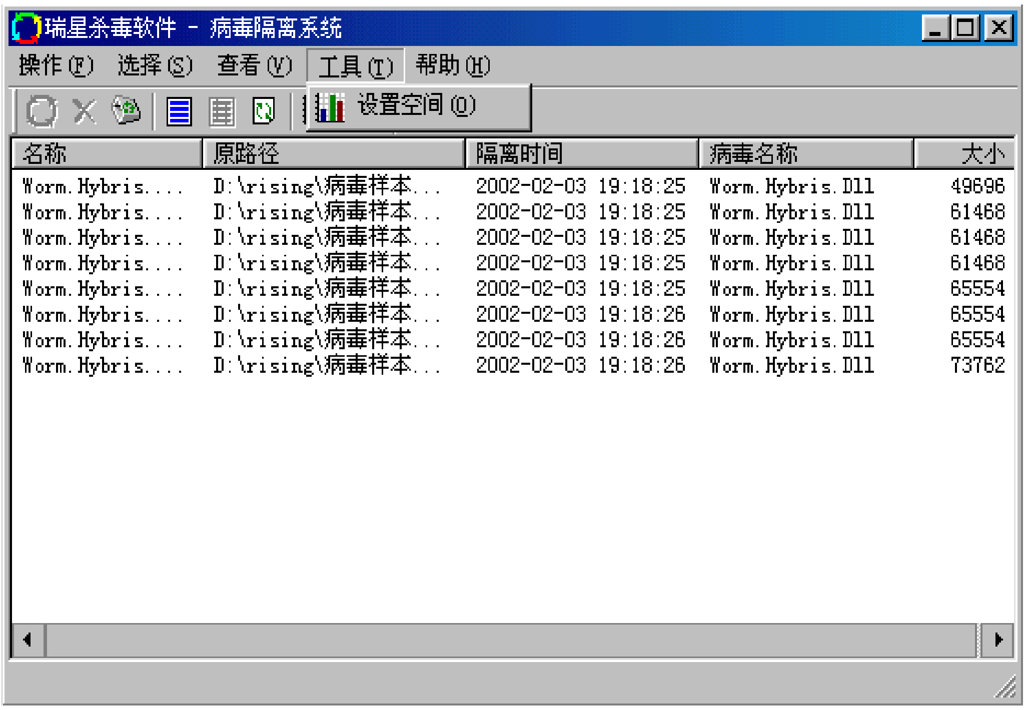


图 75

病毒隔离系统可以设置存储空间，不会因为备份文件太多而占用大量磁盘空间。

A)【隔离区容量】设置，文件替换策略：

此项如图 76 所示，分【扩展隔离区容量】和【替换最老的文件】两种。

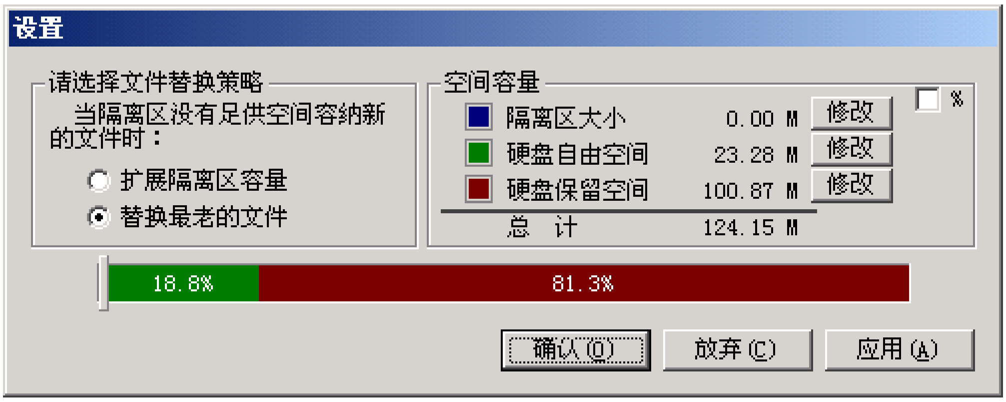


图 76

【扩展隔离区容量】：此项选择后，隔离系统容量随染毒文件增多而自动扩展，不多占用硬盘空间。

【替换最老的文件】：此项选择后，隔离系统容量固定，空间充满后自动替换最老的文件。（建议采用该方式）

【隔离区容量】设置，空间容量修改（如图 77）：

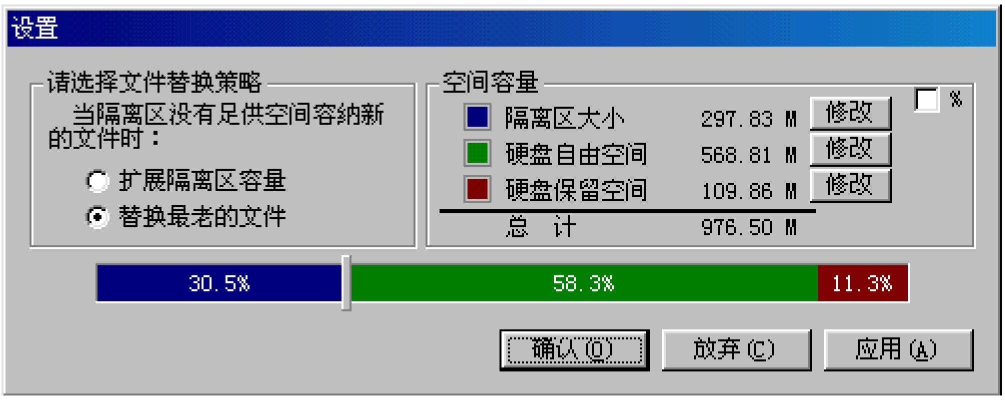


图 77

手动输入：点击【修改】按钮，修改各项空间大小（单位兆）或百分比。

隔离区大小 ：此项表示隔离系统容量，一般默认为 50 兆。

硬盘自由空间 ：此项表示硬盘剩余可用空间。

硬盘保留空间 ：此项表示保留可用空间，默认为 100 兆，防止硬盘空间被占用光。

调节滑杆 ：此项按住滑杆左右拖动，可直观更改隔离系统容量。

4.3.2 硬盘数据备份

◆ 【备份启动】项：

进入系统菜单【开始】→【程序】→【瑞星杀毒】，选择【硬盘数据备份】即可启动。

选择【开始备份】后，将会需要 10 分钟左右的时间对您的硬盘进行备份（时间长短由您硬盘大小以及文件数量决定）。（如图 78）

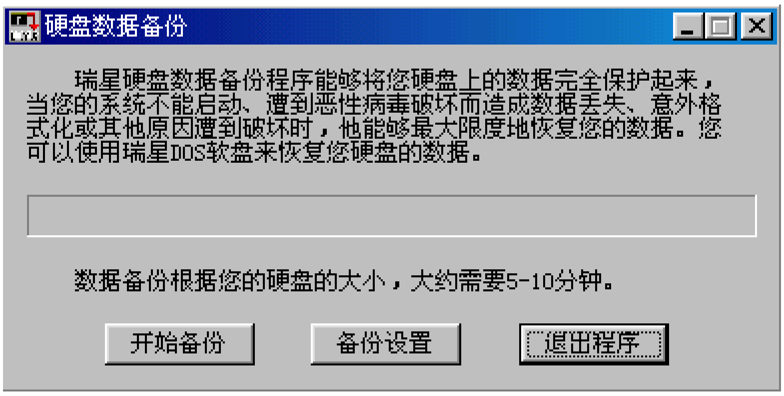


图 78

◆ 【备份设置】项：

您可以选择不备份或者指定每小时、每天、每周、每月的任何时间开始进行数据备份。通过选择【定时备份设置】后，可以保证您的数据备份是较新的，这样当你需要恢复数据时才能最大限度的减少损失。（如图 79）

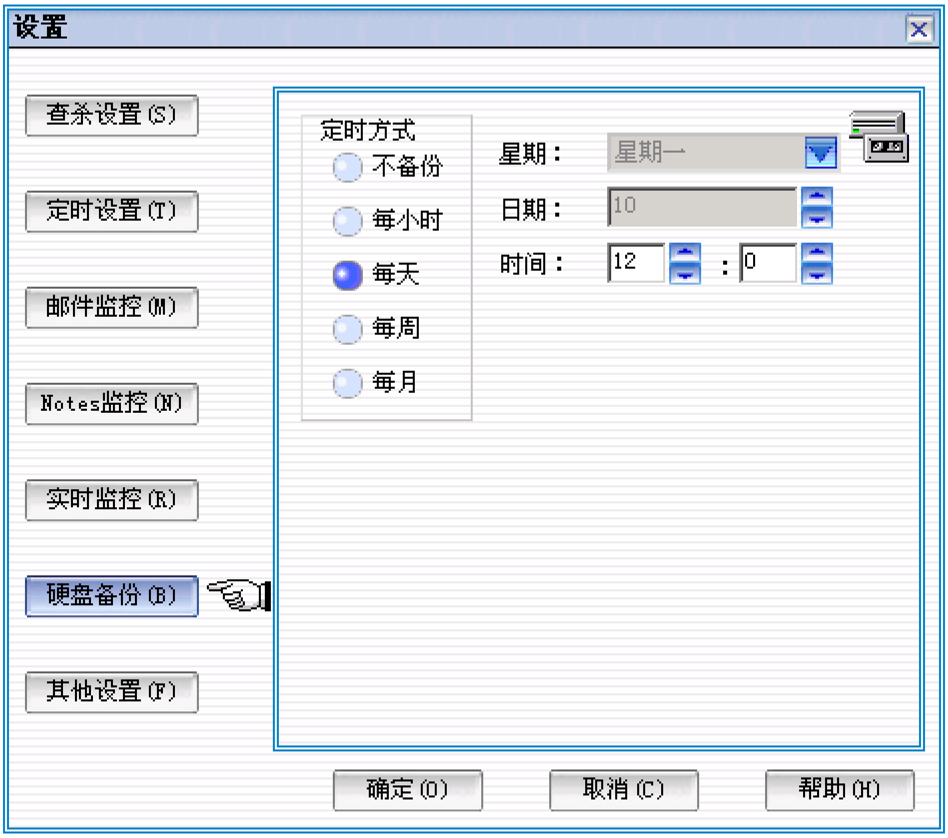


图 79

◆ 【修复】项：

如果您的硬盘数据被破坏，或者由于某种原因造成硬盘被格式化，绝大多数情况下，通过硬盘

数据修复工具将帮助您修复硬盘数据：

用瑞星 DOS 盘启动，进入瑞星 DOS 查杀程序，在【实用工具】下选择【硬盘数据恢复】，此工具将帮助您按照您最近进行的硬盘备份恢复您的硬盘数据。（详细使用方法请参看 4.4.3。）

注意：此过程可能需要比较长的时间。该修复功能不包括修复操作系统，如果您的硬盘没有被破坏，请不要使用此工具。

◆ 【空间占用】项：

硬盘备份将产生三个文件，总计占用用户的空间大约为硬盘容量的 0.02%。

4.3.3 瑞星助手

【瑞星帮助向导】可以帮助您尽快的了解瑞星软件，不仅帮助您最大限度的提高工作效率，而且给工作带来了乐趣和轻松。

◆ 【瑞星助手】的安装：安装瑞星网络版杀毒软件的同时，瑞星助手也同时被安装。

◆ 启动瑞星助手功能项：鼠标双击【瑞星助手】可以进入助手功能帮助。

◆ 【新增功能、新特性】项：此项选择后，可以帮助您尽快的了解瑞星软件新增加的一些功能，这些功能的使用可以帮助您最大限度的保护您的计算机安全。（如图 80）

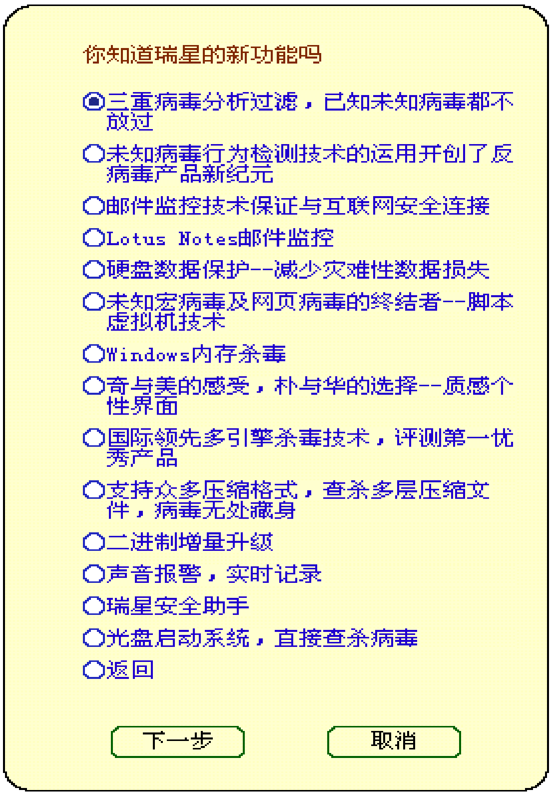


图 80

◆ 【常见问题解答】：

此项选择后，可以帮助您尽快的解答瑞星软件使用过程中可能遇到的问题。（如图 81）

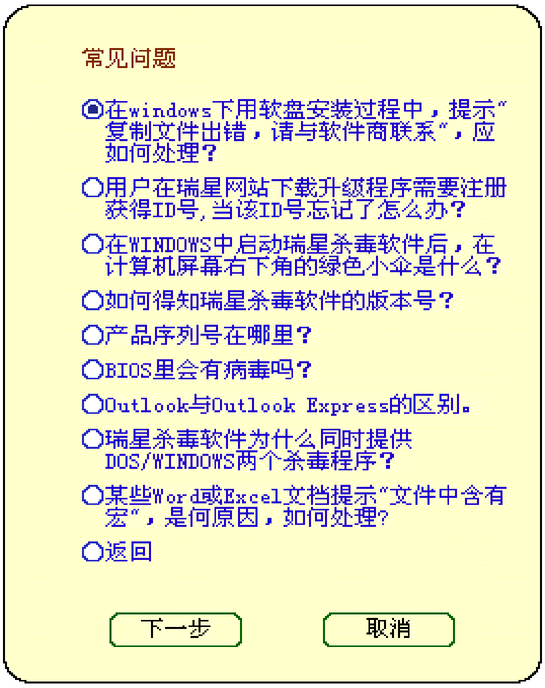


图 **81**

◆ 【启动瑞星程序】项：

此项选择后，可以快速的启动瑞星各项程序。（如图 82）

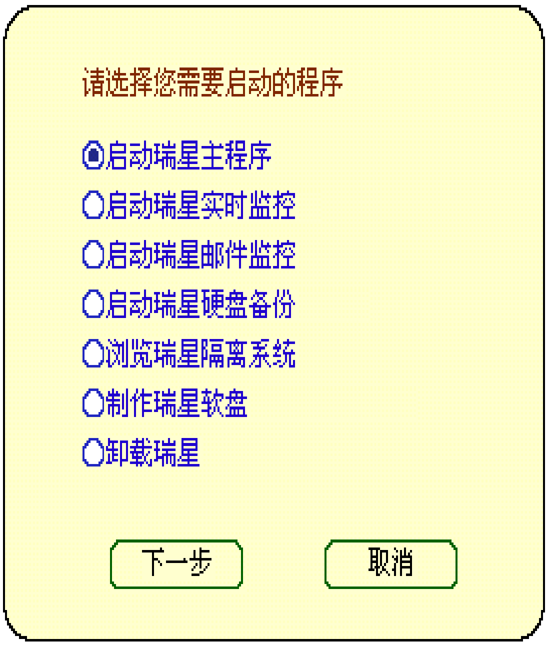


图 **82**

4.4 瑞星 DOS 盘软盘的使用

4.4.1 瑞星 DOS 软盘应用概述

瑞星网络版杀毒软件附赠瑞星杀毒软件〖DOS 盘〗杀毒软盘。瑞星杀毒软件〖DOS 盘〗是目前国内唯一DOS环境下全中文图形界面的杀毒软件。瑞星公司以绝对领先的技术，突破了Windows NT/2000 NTFS 文件系统格式的读写难题，解决了在 DOS 下对 NTFS 格式分区文件进行识别、查杀的问题。瑞星杀毒软件可以彻底、安全地查杀 FAT 和 NTFS 格式分区下的病毒，并免除了因 NTFS 文件系统感染病毒带来的困扰。

4.4.2 瑞星 DOS 盘的启动

当您在 Windows 系统环境下发现不能彻底根除的病毒（如引导型病毒，混合型病毒，特殊的网络蠕虫病毒），请用瑞星 DOS 盘启动杀毒。启动方法如下:

A)将瑞星〖DOS 盘〗的 A 号软盘插入软盘驱动器。

B)打开计算机电源或重新启动计算机，从 A 驱引导启动。

C)A 盘引导启动后，瑞星软件会自动检测您本机里瑞星程序的版本号。如版本高于软盘的版本可按回车键忽略。反之，可按提示取出 A 号盘，插入〖DOS 盘〗B 号;(如图 83)

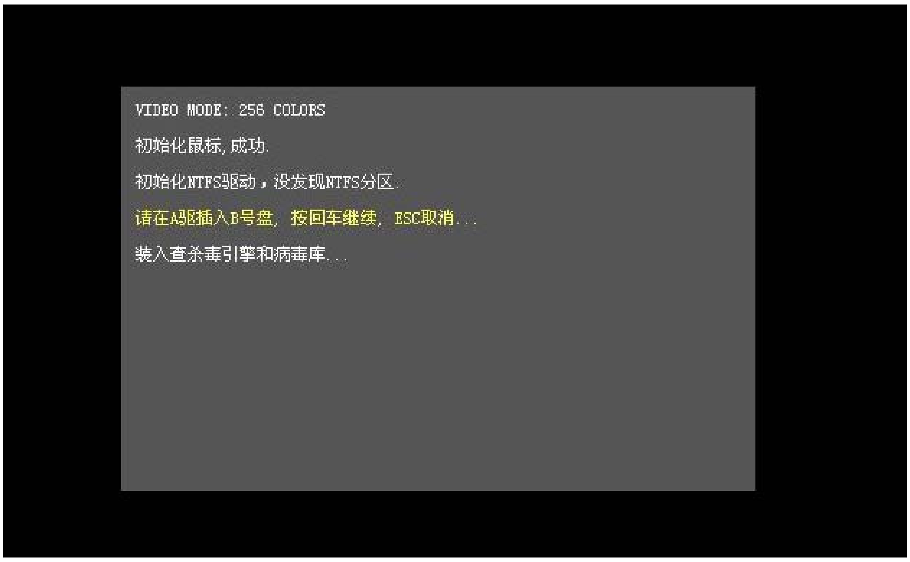


图 83

D)进入瑞星杀毒软件〖DOS 盘〗工作界面。（如图 84）



图 84

4.4.3 瑞星 DOS 盘图形界面工作方式

◆ 菜单【快速查杀步骤】项

A）进入 DOS 盘的查杀毒界面（如图 84）。

B）在查毒/杀毒界面下选择需要查杀的目录（缺省状态下扫描本机所有硬盘）。注：A：指 A 软盘驱动器； X，Y，Z：指硬盘分区，可分别选择查杀。

C）选定目标后，用鼠标点击查毒按钮或按<ENTER>键即开始查毒。

D）用鼠标点击<杀毒>按钮，或按<TAB>键将光标移动到<杀毒>按钮后，按<ENTER>键即可本机直接杀毒。

E）在查杀毒过程中可以用鼠标直接点击<暂停>按钮来暂停查杀病毒，按<继续>后继续扫描。

按【完成】按钮结束本此查杀病毒，在查杀结果栏中会显示查杀结果。（如图 85）



图 85

F）用鼠标或用<TAB>键，<上/下/左/右>键选择其他驱动器和路径进行查杀病毒。

◆ DOS 盘杀毒设置

A）『查毒/杀毒』页中有如下选择和功能：

查毒：扫描磁盘检查病毒，并将病毒列表在查杀结果栏中显示

杀毒：扫描磁盘清除病毒，并将病毒列表在查杀结果栏中显示

退出：直接退出瑞星杀毒软件〖DOS 盘〗。

B）在『功能设置』页中有如下功能选项：（如图 86）



图 86

用键盘的上、下键移动光标或直接用鼠标点击选项进行选定/取消。

【仅查程序文件】项：选定后仅扫描程序文件，取消后将扫描所有文件。

【查杀未知 WINDOWS 病毒】项：选定后增加对未知 WINDOWS 病毒的扫描。

【查压缩文件】项：选定后增加对压缩文件的扫描。

【备份病毒有关文件】项：选定后在杀毒过程中会备份带毒文件，您可以在〖WINDOWS 版〗中恢复。

【查引导区】项：选定后查引导区病毒。

【查杀未知 DOS 病毒】项：选定后查未知 DOS 病毒。

【杀毒前询问用户】项：选定后在杀毒前将提示用户确认处理方式。

【退出】项：直接退出瑞星杀毒软件〖DOS 盘〗。

功能设置的具体信息也可参看 4.2.2 的设置。

C）在【实用工具】页中有如下选择和功能：（如图 87）



图 87

【提取硬盘引导区信息】项：此功能用于提取您的硬盘引导区信息。如果您认为您的引导区有问题或者怀疑被病毒感染，您可以通过此工具提取您的硬盘引导区信息，通过 E.MAIL 发送或提供样本给瑞星公司进行分析。

【硬盘数据恢复】：当您的机器硬盘被破坏时，紧急修复硬盘的工具。如果您在 Windows 下做了硬盘数据备份，可以选择 【实用工具】→【硬盘数据恢复】项，将为您查找此备份提示出硬盘数据信息并通过此备份修复您的硬盘（此过程可能需要比较长的时间）。

注意：如果您的硬盘没有被破坏，请勿使用此工具。

【退出】：直接退出瑞星杀毒软件〖DOS 盘〗。

4.4.4 瑞星〖DOS 盘〗软盘升级

在瑞星网络版进行版本升级的同时，您可以将瑞星 DOS 盘杀毒软件同时进行升级，瑞星在 WINDOWS 操作界面下为您提供了单独的瑞星杀毒软件 DOS 盘升级工具(详细操作见 7.4)。

注意：

1. 严禁将 A 盘格式化。

2．禁止将下载得到的升级程序拷贝到原盘中。

3．禁止用任何工具（如 Scandisk、Defrag、NU、Pctools 等）对 DOS 原盘进行检测、修改、修复等操作。

4．升级程序不能在 DOS 和 Windows 3.X 环境下运行。

第五章 病毒实时监控

5.1 实时监控概述

避免因病毒的破坏造成不必要的损失的关键在于防范。人为的防范必然要投入很大的精力和人力，给工作造成了很大的压力。瑞星中小企业版的实时监控系统采取统一管理的监控体系，使整个网络始终处于一个整体的监控环境下，任何一个安全漏洞管理员都可以及时的发现远程处理。

在安装【瑞星杀毒软件中小企业版】的同时，实时监控程序将自动安装到当前计算机系统中，并在【开始】/【程序】/【瑞星杀毒】程序文件夹中建立名为【瑞星实时监控】的快捷方式。实时监控程序运行时，将监控本机文件的所有操作，一旦发现病毒，将按照已设定好的处理方式处理病毒，并将结果上报给管理员管理控制台，使管理员能最短时间内掌握整个网络的病毒发作和传播情况。

5.1.1 启动实时监控

方法一：在安装结束后，选择【运行实时监控】，实时监控会自动启动。(如图 88)



图 88

方法二：在 Windows 桌面状态下，依次进入【开始】/【程序】/【瑞星杀毒】，选择【瑞星实时监控】即可启动。

方法三：在【瑞星管理员管理控制台】中，选定要启动实时监控的计算机，点击快捷按钮。

方法四：启动瑞星网络版杀毒软件主程序，在【工具】菜单下选择[开/关实时监控](如图 89)，若此时实时监控未启动，则启动实时监控，若此时已启动，此按钮将关闭实时监控。



图 89

启动实时监控后，随即在系统托盘区（位于桌面任务栏右侧显示时钟的区域）出现小雨伞标志（）。“绿色打开”代表监控有效状态，“黄色打开”代表用户选择了【关闭文件监控】或【关闭内存监控】，“红色收起”代表监控关闭状态。

5.1.2 设置实时监控

用鼠标右键单击小雨伞，选择【设置】（如图 90）可调出设置窗口。您可以通过对（图 91）实时监控设置相应选项的调整来确定您合适的监控策略。



图 90

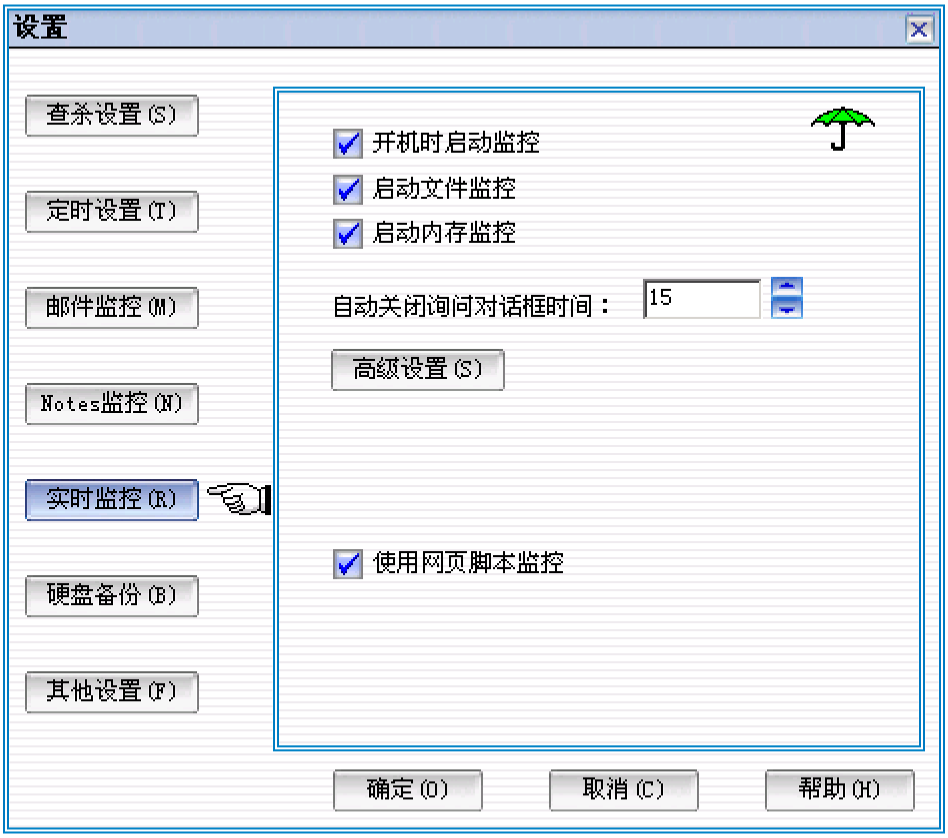


图 91

在【实时监控】属性页中，选择【开机时启动监控】，即可在每次启动计算机时自动运行瑞星杀毒软件实时监控程序。选择【使用网页脚本监控】后，瑞星杀毒软件即可在用户浏览网页时在打开网页之前截获某些恶意脚本，完全免除了用户浏览网页的后顾之忧。在【自动关闭询问对话框时间】中，当实时监控程序发现病毒时，如果【高级设置】中设定的【发现病毒后的处理方式】为【询问后处理】则会弹出警告窗口并停留一段时间直至用户做出选择，停留的时间长短由该项设置所设定（单位为秒），如果超过设定时间用户还没有进行操作，则实时监控程序将直接清除该病毒。

新特性：网页脚本监控。

强烈建议：请选中【启动文件监控】和【启动内存监控】，这样实时监控就始终处于打开状态，一旦发现病毒就会及时报警。（如图 92）



图 92

5.1.3 实时监控工作中的提示

（1）文件监控发现病毒时的提示（如图 93）：

您可以选择【杀毒】、【放弃访问】或者【删除文件】。如果您不选择，此对话框会自动关闭。

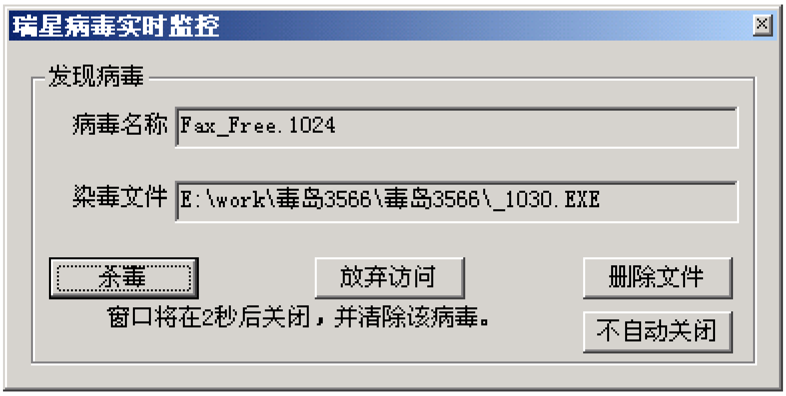


图 93

（2）内存监控发现病毒时的提示（如图 94）：

您可以选择【拒绝运行退出程序】从而终止程序的运行，或者选择【剥离病毒安全运行】从而继续运行程序。



图 94

（3）内存监控发现木马、黑客程序时的提示（如图 95）：

因为木马和黑客程序不包含有用的程序，所以只提供了【拒绝运行退出程序】的选项。



图 95

5.1.4 禁止实时监控

用鼠标右键单击系统托盘（位于 Windows 窗口任务栏中显示时钟的区域）中的【瑞星反病毒实时监控】图标（绿色小雨伞标志），选择【关闭文件监控】和【关闭内存监控】，这时【瑞星反病毒实时监控】图标由“绿色打开”变为“红色收起”，此时实时监控程序并未真正退出，您仍然可以选择【开启文件监控】和【开启内存监控】来启动实时监控。如果仅选择了【关闭文件监控】和【关闭内存监控】其中一项，【瑞星反病毒实时监控】图标由“绿色打开”变为“黄红打开”。

5.1.5 退出实时监控

方法一：用鼠标右键点击系统托盘区中的瑞星实时监控程序图标（形如小雨伞），再选择【关闭实时监控】。

方法二：在瑞星杀毒软件主界面中，选择【工具】→【开/关实时监控】，若此时实时监控已启动，即可关闭实时监控。

提示：管理员应该在管理控制台中给客户的实时监控加入密码，避免随意关闭。

5.2 邮件监控

5.2.1 启动邮件监控

在 Windows 窗口中，选择【开始】→【程序】→【瑞星杀毒】→【邮件监控】（如图 96）：

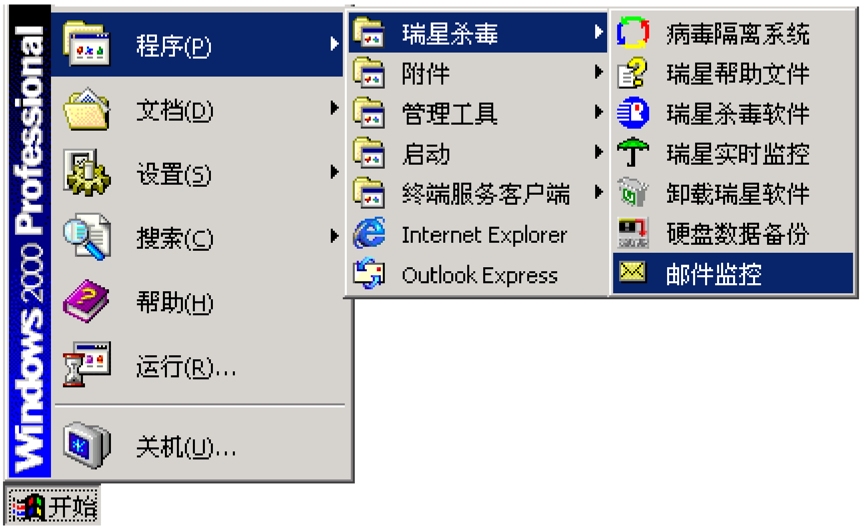


图 96

5.2.2 【邮件监控】设置说明

在瑞星杀毒软件主程序中，选择【设置】→【选项】→【邮件监控】，即可设置【邮件监控】（如图 97）。

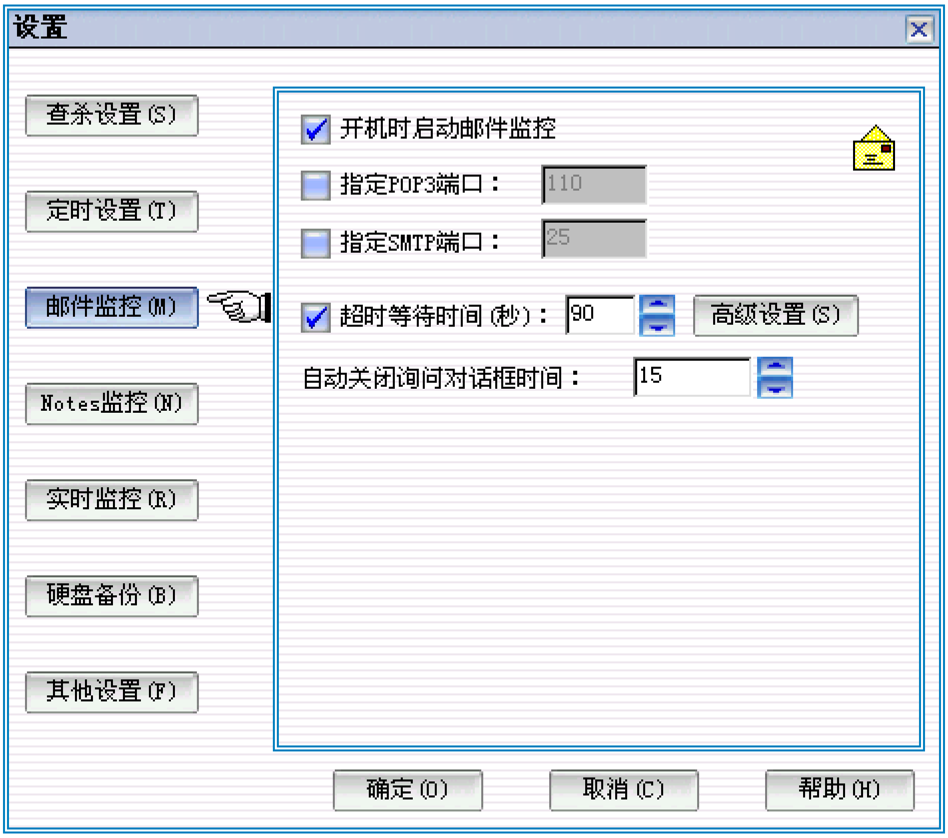


图 97

开机时启动邮件监控：每次开机自动启动邮件监控程序。

指定 POP3 端口：默认邮件端口是 110，某些时候这个端口会被其它程序占用（例如代理程序或者其它杀毒软件），您可以通过指定其它端口解决这个问题。

指定 SMTP 端口：默认邮件端口是 25，某些时候这个端口会被其它程序占用（例如代理程序或者其它杀毒软件），您可以通过指定其它端口解决这个问题。

超时等待时间：有时候网络忙会导致邮件一时无法接收下来，设定一个超时，可以使我们早些放弃，不必要浪费过多的时间在等待上。默认为 90 秒。

自动关闭询问对话框时间：当邮件监控发现病毒，而您在高级设置中又是选择的询问后处理时，会弹出对话框询问用户。如果这时候用户不在场，询问对话框就会阻塞邮件的接收。设置一个自动关闭询问对话框的时间，可以保证不会发生这样的情况。默认的自动关闭时间为 15 秒。

5.2.3 邮件监控工作中的提示

（1）发送邮件提示

当您选择发送邮件的时候，邮件监控会自动进行代理工作（如图 98），显示发送邮件进度，选择【隐藏】可以隐藏该对话框，但是不会影响工作。



图 98

（2）接收邮件提示

当您选择接收邮件的时候，邮件监控会自动进行代理工作（如图 99），显示接收邮件进度，点击【隐藏】可以隐藏此对话框。但是不会影响工作。

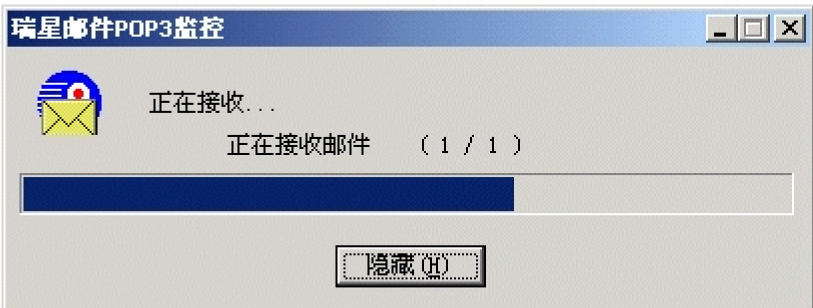


图 99

（3）发现病毒的提示

邮件监控首先把要发送的邮件保存到瑞星安装目录下的一个目录，并向用户显示对应的邮件信息和病毒信息（如图 100）。用户可以自己处理该邮件。

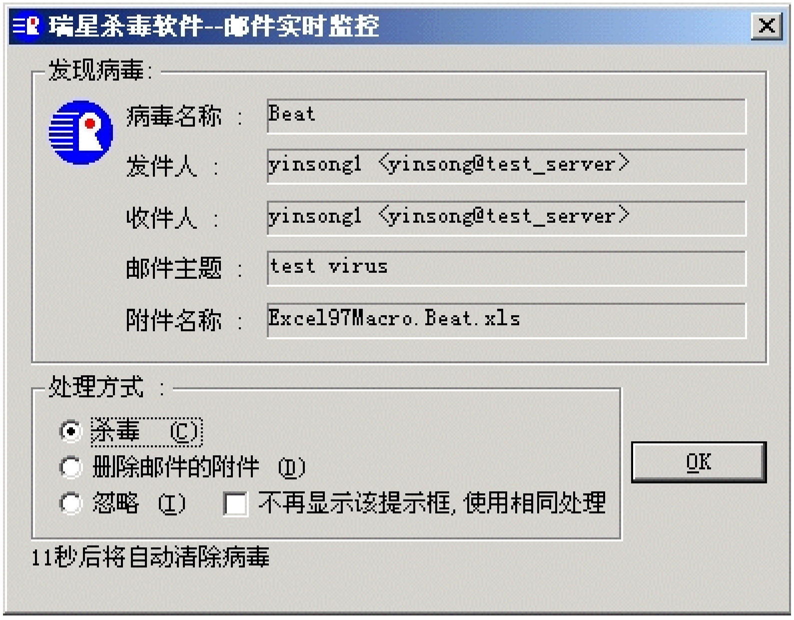


图 100

如果发送过程中发现病毒则不发送该邮件到邮件服务器。邮件监控将产生报告（如图 101）：

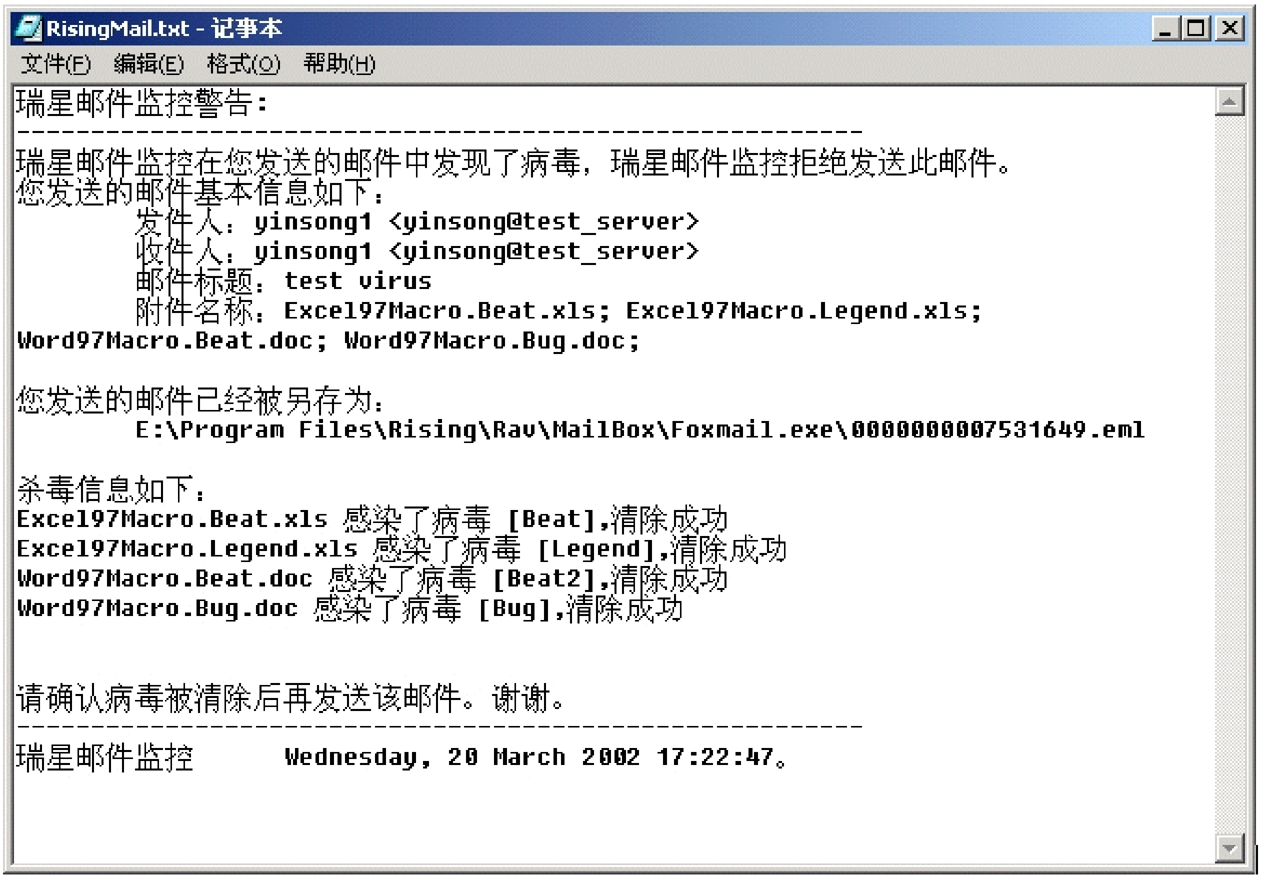


图 101

在接收过程中如果发现邮件中包含病毒，邮件的主题将会有【瑞星警告】等信息，并在附件中会多出一个文本文件，记载着瑞星邮件监控对该邮件的处理信息（如图 102）：

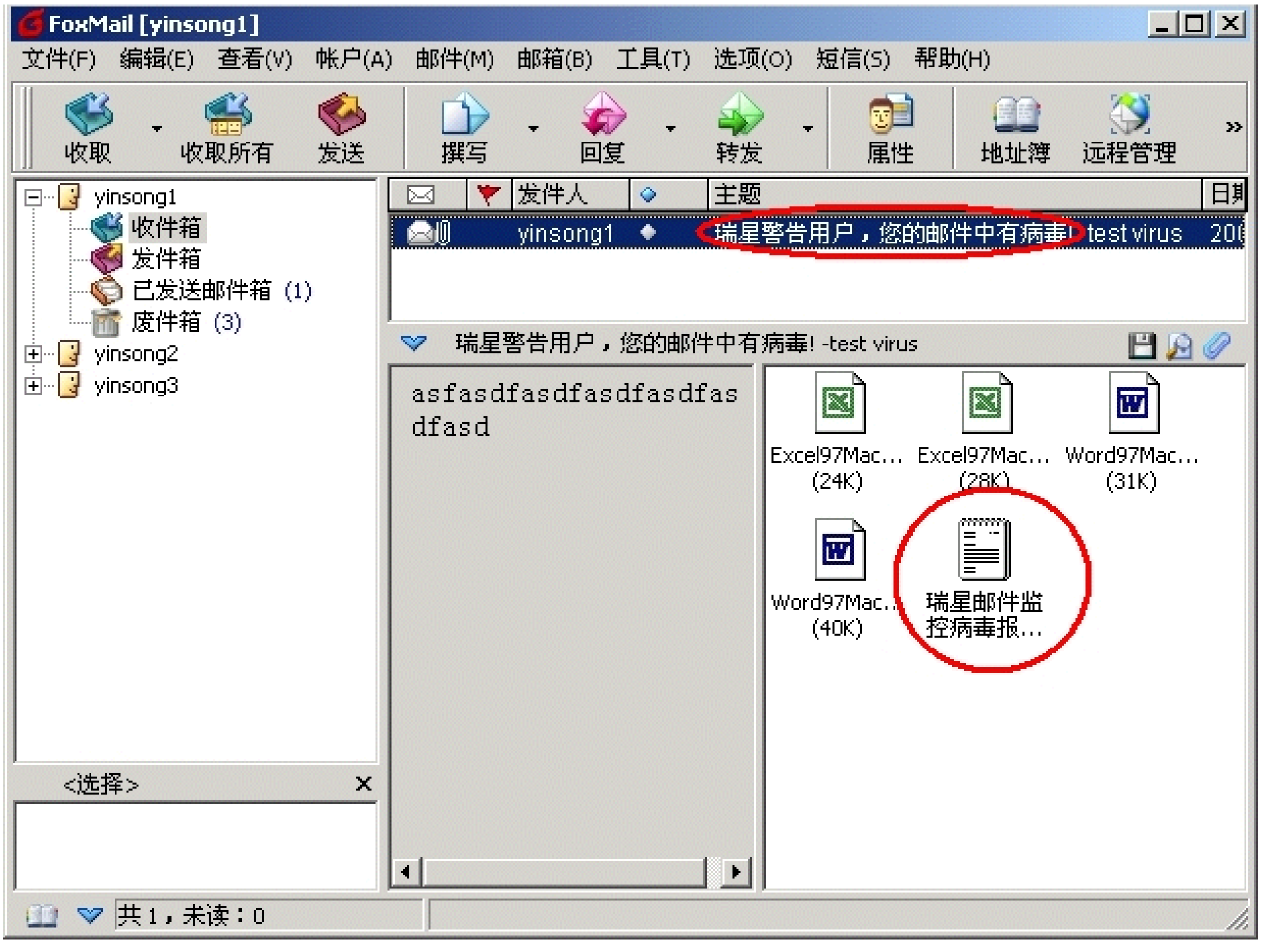


图 102

（4）发现未知程序发送邮件的提示

当发现未知程序发送邮件，瑞星邮件监控会立刻报告用户，让用户选择是否同意使用该程序发送该邮件（如图 103）：



图 103

如果用户选择【同意发送】,【瑞星邮件实时监控】会询问用户【下次发现该程序发送邮件时是

否不再提示【(如图 104)：

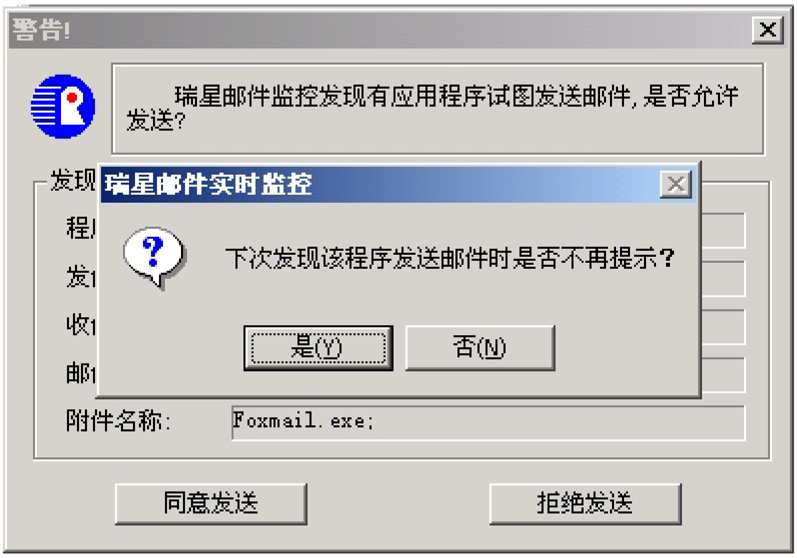


图 104

5.2.4 退出邮件监控

方法一：用鼠标右键点击系统托盘区中的瑞星邮件实时监控程序图标，再选择【退出邮件监控】。
方法二：在瑞星杀毒软件主界面中，选择【工具】→【开/关邮件监控】，若此时邮件监控已启动，即可关闭邮件监控。

5.3 Notes 监控

5.3.1 安装 Lotus Notes 监控

如果您安装了 Lotus Notes,可以通过【Notes 监控设置】对 Lotus Notes 邮件监控进行设置（如图 105）。瑞星安装程序会把 Lotus Notes 监控系统自动安装到您得计算机中。

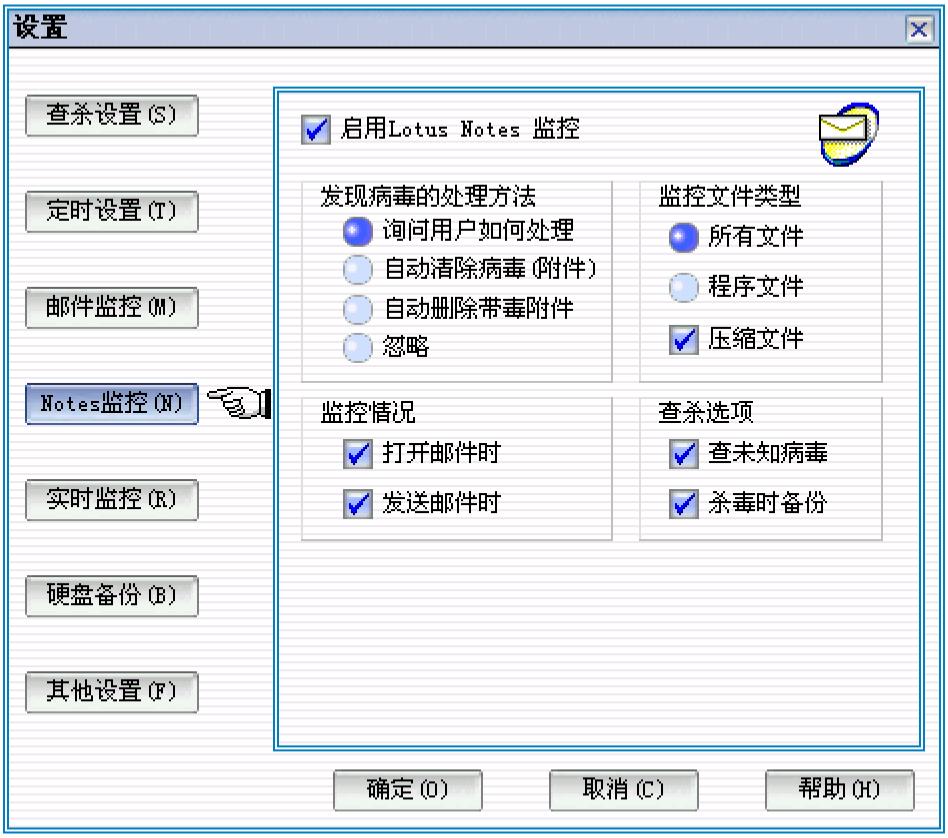


图 **105**

5.3.2 设置 Lotus Notes 监控

- 启用 Lotus Notes 监控：选中该项后，则对 Lotus Notes 系统进行监控。
- 发现病毒的处理方法：

  A）【询问用户处理】：此选项被选择后，查毒过程中发现病毒将询问用户如何处理，建议用户使用【询问后处理的方式】。

  B）【自动清除病毒（附件）】：此选项被选择后，查毒过程中发现附件带毒后将直接清除附件中病毒。

  C）【自动删除带毒附件】：此选项被选择后，查毒过程中发现附件带毒后将直接删除带毒附件。

  D）【忽略】：此选项被选择后，查毒过程中发现病毒将不作任何处理继续进行扫描。
- 监控文件类型

  A）【所有文件】：选择后将监测任何格式的文件。

  B）【程序文件】：选择后将监测EXE、COM、SYS、VXD、DRV、DLL、BIN、OVL、386、SRC、HTM、HTML、FON、VBS、DOC、DOT、XLS、XLT等扩展名的文件。

  C）【压缩文件】：选中该选项后将对压缩文件进行病毒扫描。
- 监控情况

  【打开邮件时】：选中该项后在打开 Lotus Notes 邮件时将进行病毒扫描。

【发送邮件时】：选中该项后在发送 Lotus Notes 邮件时将进行病毒扫描。

◆ 查杀选项

【查未知病毒】：此选项被选择后可检测出携带未知病毒的邮件。

【杀毒时备份】：此项选中后在杀毒前,将会把所有清除或删除的染毒文件备份在【病毒隔离系统】中。

注：对 Lotus Notes 邮件设置更改后，需要重新启动 Lotus Notes 设置才能生效。

第六章 全网安全管理

6.1 管理控制台概述

【瑞星管理员管理控制台】是在网络上集中管理所有安装瑞星杀毒软件的计算机的管理工具。通过管理控制台可以远程管理网络中的任何一台计算机中的杀毒软件。网络上任何一台计算机的病毒警告信息都能在管理控制台得到汇总，通过管理控制台也能直观地查看网络上所有计算机当前实时监控、查杀毒、当前版本等状态。管理控制台能对远程计算机安装杀毒软件和管理控制台，让管理控制台自由移动到管理员认为合适的计算机上去。管理员通过管理控制台的操作就能对网络上所有计算机进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个网络外围建立一面坚实的网络病毒防护系统。

6.2 管理控制台的启动

启动已经安装瑞星管理员管理控制台的机器，依次进入【开始】/【程序】/【瑞星杀毒】，选择【瑞星管理员管理控制台】或者双击桌面管理员图标【瑞星管理员控制台】进入登录界面（如图 106）

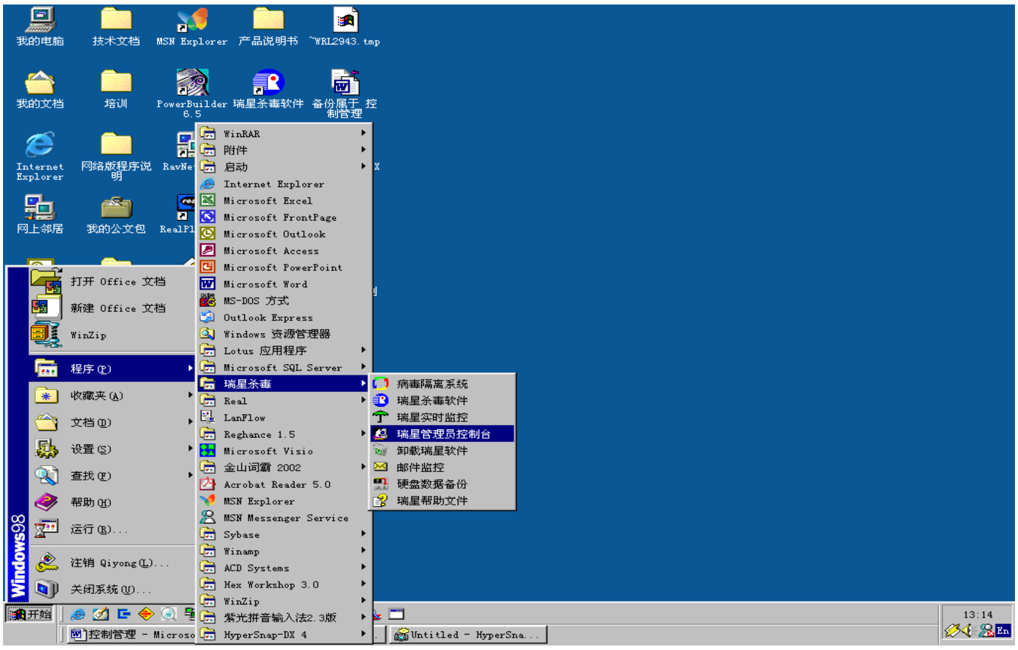


图 106

输入用户名和密码后，单击【确定】进入管理控制台管理界面（如图 107）

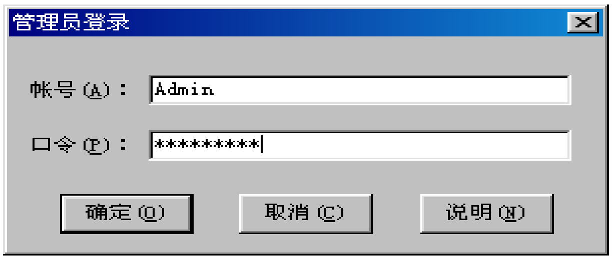


图 107

提示：默认的用户名是“ADMIN”，请保存好管理员密码，如果意外丢失请和瑞星公司技术服务部取得联系。

6.3 控制台面板介绍

瑞星管理员管理控制台（如图108）分为4个部分：功能菜单项、组管理界面、计算机列表栏、病毒信息列表栏。

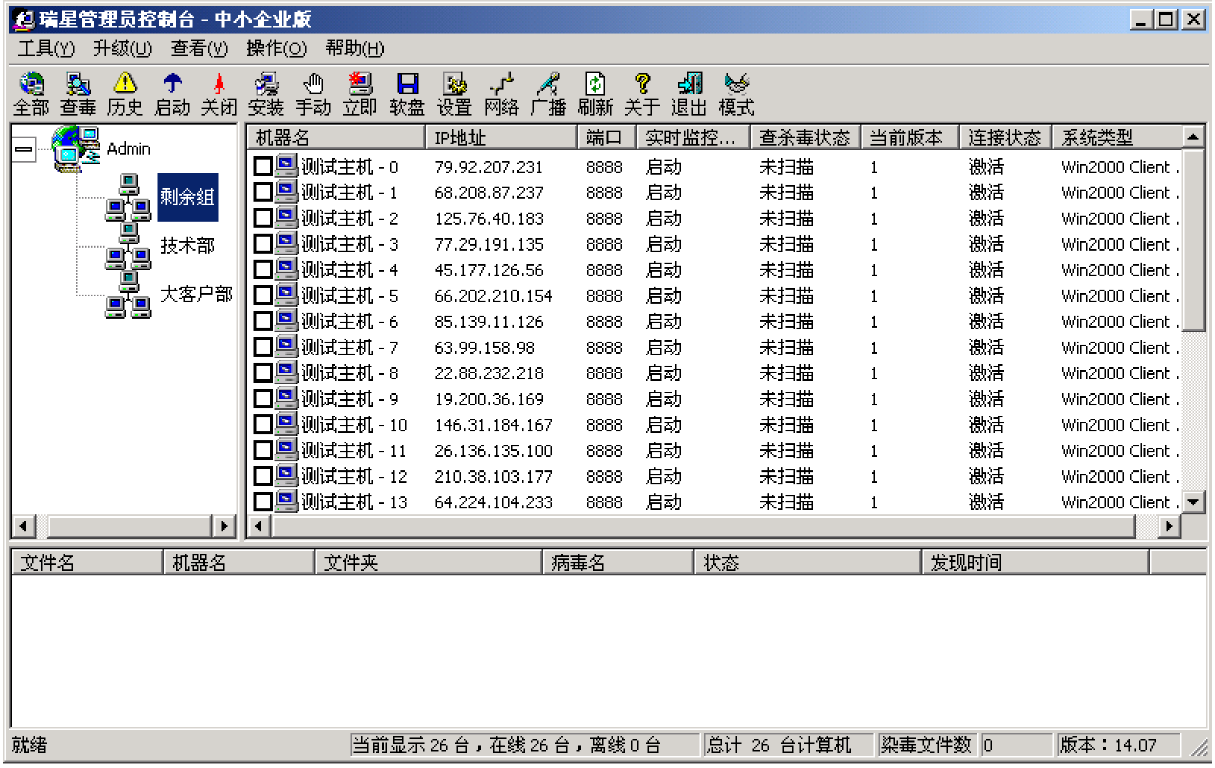


图108

6.3.1 功能菜单项

点击该栏的功能图标即可完成管理控制的多项重要功能。（如图109）



图109

- 【工具】菜单：（如图110）

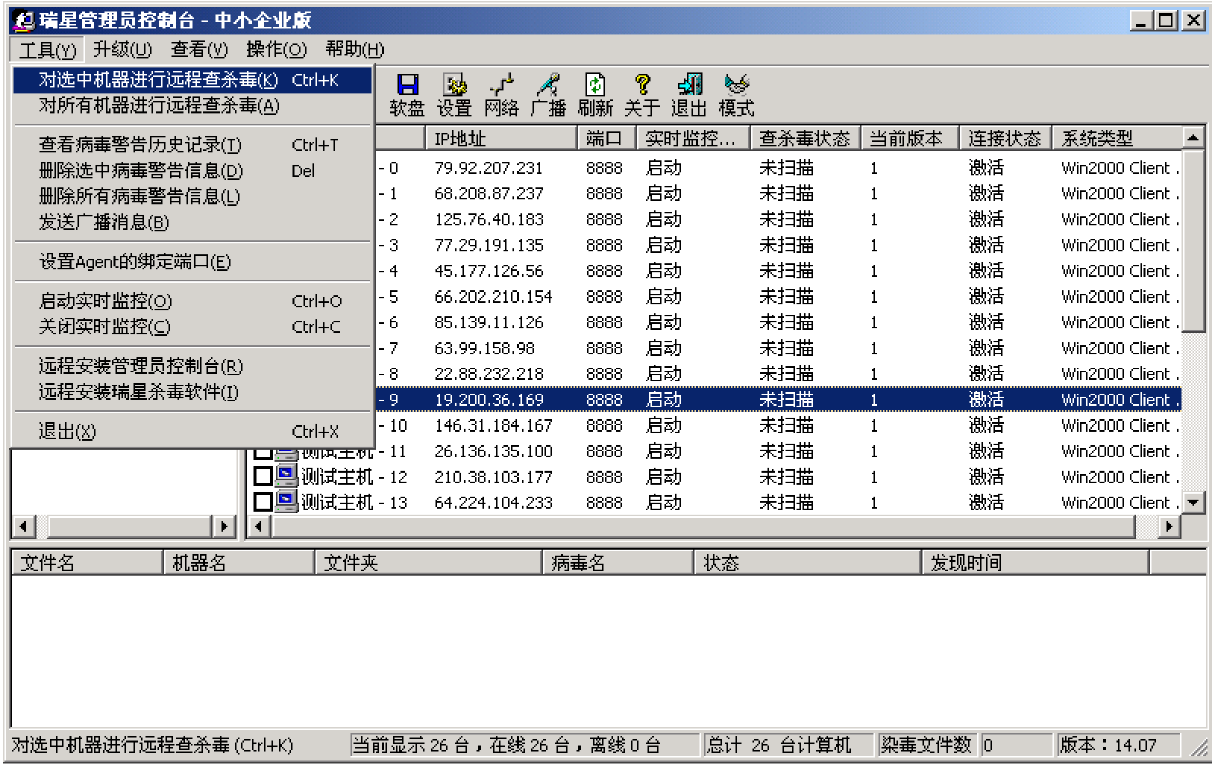


图110

A)【对选中机器进行远程查杀毒】：选中一台计算机或多台计算机，然后选中该菜单项，即可对所选中的计算机进行远程查杀毒。

B)【对所有机器进行远程查杀毒】：选中该菜单项，即可对所有计算机进行远程查杀毒。如果此时有计算机处于关机状态，该机开机后即自动进行查杀毒。

C)【查看病毒警告历史记录】：选中该菜单，显示所有的病毒警告信息。

D)【删除选中病毒警告信息】：在【病毒列表信息栏】选中需删除的病毒信息后，单击该选项即可删除该条信息。

E)【删除所有病毒警告信息】：选中该菜单即可删除所有【病毒列表信息栏】中的病毒信息。

F)【发送广播信息】：选中该菜单，即可对选中的机器发送广播短信，默认为所有机器。

G)【设置Agent的绑定端口】：选中该菜单后，即可对瑞星后台程序选用的端口重新设定。

H)【启动实时监控】：选中需要执行该操作的机器，单击该菜单，即可开启目标机器的实时监控程序。

I)【关闭实时监控】：选中需要执行该操作的机器，单击该菜单，即可关闭目标机器的实时监控程序。

J)【远程安装管理员管理控制台】：选中需要安装管理控制台程序的机器，单击该菜单，即可给目标机器安装移动管理控制台。

K)【远程安装瑞星杀毒软件】：单击该菜单，在弹出的对话框中选中目标机器，即可远程对该机器实现远程安装。

L)【退出】：单击该项，即可退出瑞星管理员管理控制台程序。

◆ 【升级】菜单：（如图111）

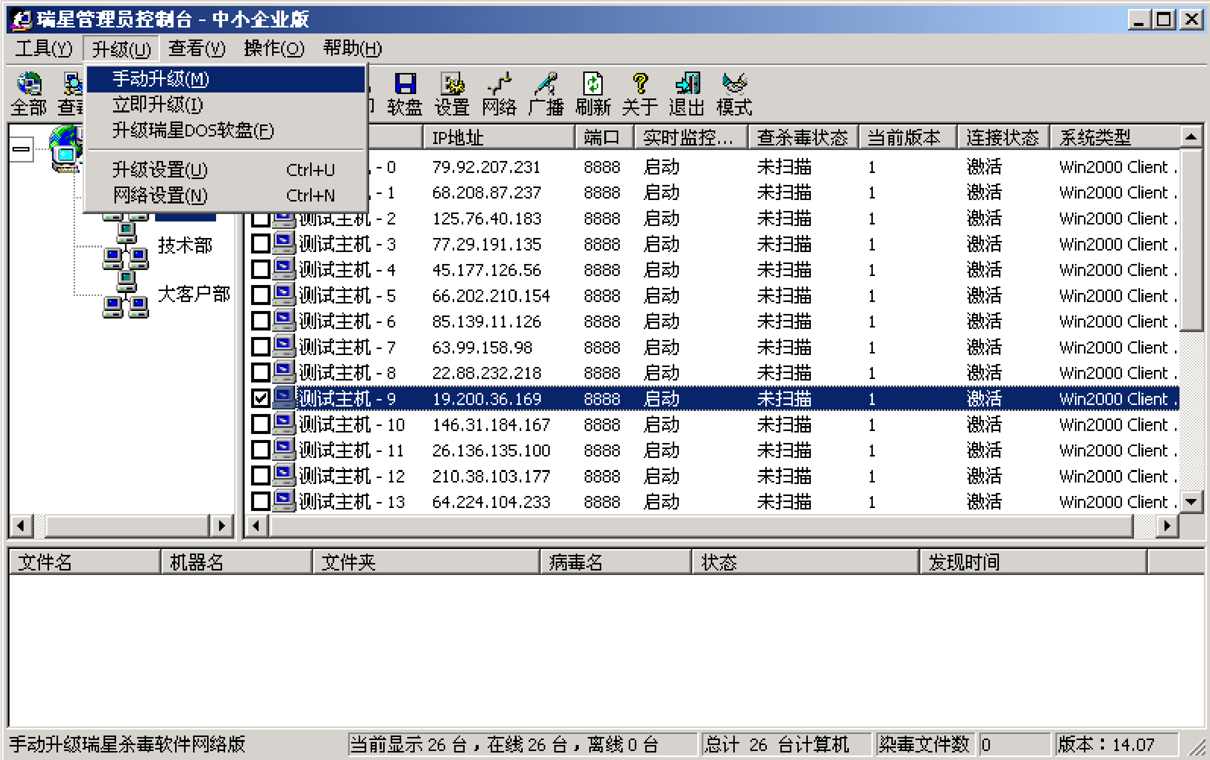


图111

A)【手动升级】：选中该项后，在弹出的【打开】对话中选择升级包程序，单击打开即可对全网所有机器进行升级。

B)【立即升级】：选中该项后，瑞星程序将自动连接瑞星网站进行全网的升级。

C)【升级瑞星DOS软盘】：在软驱中插入瑞星网络版附带的dos盘后，选中该项，即可将DOS盘程序升级到当前本机最高版本。

E)【升级设置】：瑞星网络版支持多种升级方式，该部分详细介绍请参见“第七章.版本升级”。

F)【网络设置】：服务器连接Internet的方式各不相同，请在这里选择适合您的方式。

（升级详细介绍请参见“第七章.版本升级”）

◆ 【查看】菜单：（如图112）

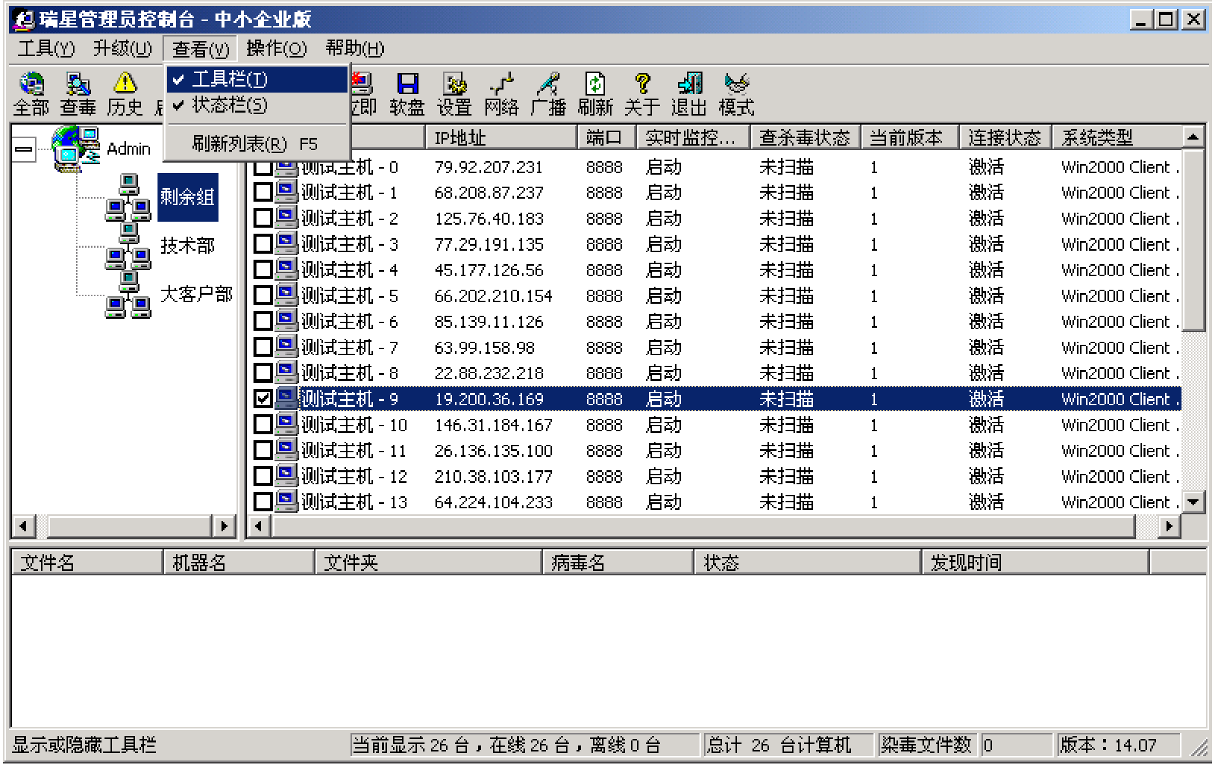


图112

A)【工具栏】：选中该选项后，会在管理控制台上端列出一些快捷按钮，功能与各所属菜单项内的选项功能相同，如图所示。工具栏上的快捷按钮主要有：（如图 113）



图 113

【全部】：对所有在瑞星管理控制台中注册过的计算机进行远程查杀毒；

【查毒】：对选中计算机进行远程查杀毒；

【历史】：显示指定用户的病毒警告历史记录；

【启动】：通过瑞星管理员管理控制台可以启动选中计算机的【实时监控】程序；

【关闭】：通过瑞星管理员管理控制台关闭选中计算机的【实时监控】程序；

【安装】：对选中的计算机进行远程安装瑞星管理员管理控制台；

【手动】：对瑞星杀毒软件进行手动升级；

【立即】：根据升级设置立刻进行智能升级（如果设置中选择不使用自动设置，选中该按钮后，会默认为自动下载,自动升级）；

【软盘】：升级 DOS 盘瑞星杀毒软件；

【设置】：对瑞星杀毒软件进行自动升级设置；

【网络】：对局域网连接到互联网的方式进行设置；

【广播】：向客户端发送广播；

【刷新】：重新获取整个局域网内可以管理的计算机列表。

【关于】：显示瑞星管理员管理控制台的版本等信息。

【退出】：退出瑞星管理员管理控制台。

【模式】：切换到/管理模式。

B)【状态栏】：在病毒信息列表栏下方，动态显示管理控制台的当前状态信息。（如图 114）



图 114

C)【刷新列表】：选中该选项后，将重新获取整个局域网内可以管理的计算机列表信息。

◆　『操作』菜单：（如图 115）

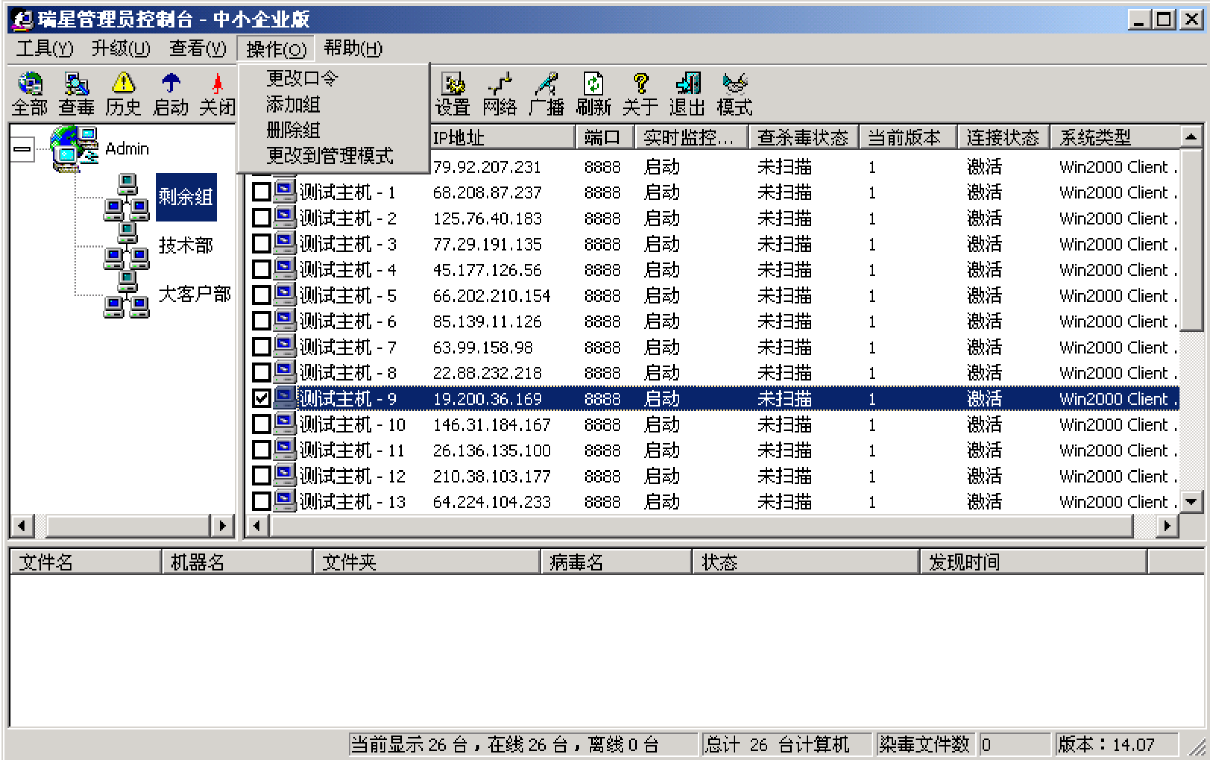


图115

A)【更改口令】：选中该项后，即可对您Admin帐号的密码进行设置和更改。（如图116）

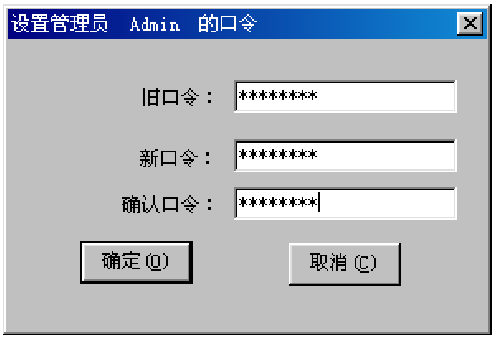


图116

B)【添加组】：选择该项后，即可在【组管理界面】里添加新组。

C)【删除组】：选中您需要删除的组，单击该项菜单栏即可删除。

D)【更改到管理模式】：选中该项即刻切换到【管理模式】。

◆　『帮助』菜单：（如图117）

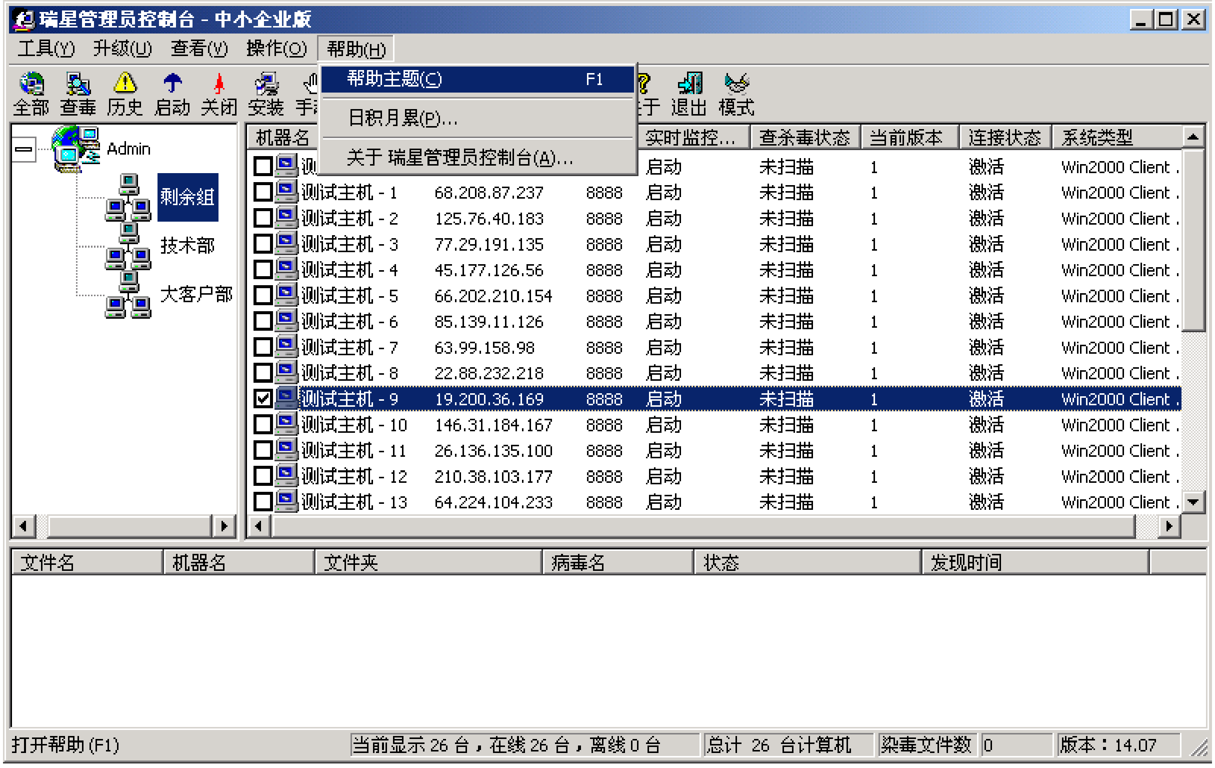


图117

A)【帮助主题】：单击该项，获取相关帮助。

B)【日积月累】：单击该项，您可以获取有关病毒方面的小常识和有关的资料。

C)【关于瑞星管理员管理控制台】：单击该项，您可以查看相关信息。

6.3.2 组管理界面

一种基于用户分组管理的功能界面，在这里我们可以简单的创建组，并为该组添加相应成员，关于该部分的详细介绍请参见“6.5 用户管理”节。（如图118）

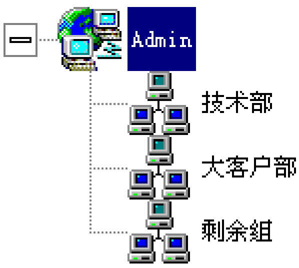


图118

6.3.3 计算机列表栏

在该列表栏中（如图119），显示注册过的机器名、IP地址、端口、实时监控状态、查杀毒状态、当前版本、连接状态以及系统类型。并支持为选中的机器设置客户端口令。该列表栏支持鼠标右键

功能（包括:【全选】、【全不选】、【反选】、【设置客户端口令】等）。

关于该部分的详细的介绍请参见“6.4 远程控制”节。

机器名	IP地址	端口	实时监控...	查杀毒状态	当前版本	连接状态	系统类型
测试主机 - 0	79.92.207.231	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 1	68.208.87.237	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 2	125.76.40.183	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 3	77.29.191.135	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 4	45.177.126.56	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 5	66.202.210.154	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 6	85.139.11.126	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 7	63.99.158.98	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 8	22.88.232.218	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 9	19.200.36.169	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 10	146.31.184.167	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 11	26.136.135.100	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 12	210.38.103.177	8888	启动	未扫描	1	激活	Win2000 Client .
测试主机 - 13	64.224.104.233	8888	启动	未扫描	1	激活	Win2000 Client .

图119

6.3.4 病毒信息列表栏

该列表栏（如图 120）显示局域网上所有发现的病毒信息，包括文件名、文件所在的计算机名、文件所在的文件夹、病毒名、病毒的状态以及发现该病毒的时间。

该列表栏支持鼠标右键功能（包括:【全选】、【全不选】、【反选】、【删除选中病毒警告信息】以及【删除所有病毒警告信息】）。

文件名	机器名	文件夹	病毒名	状态	发现时间
13.49.00....	WANGXIULIANG	e:\	Script.Exploit.H...	发现病毒	2002-05-17 16:20:02

图 120

注意：当在病毒信息栏出现“请双击”提示时，您可以双击该提示查看具体的病毒信息。

6.4 远程控制

6.4.1 远程查杀

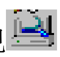
在瑞星管理员管理控制台上可以任选一台或多台计算机进行远程查杀毒，在机器列表栏选择需要查杀的机器名，点击【查毒】按钮或工具菜单栏下的【对选中的计算机进行远程查杀毒】后会弹出瑞星杀毒软件中小企业版远程查杀毒对话框。（如图121）单击查毒或杀毒即可完成相关操作。同时在目标客户端系统右下角会出现图标，表示其正在被执行远程杀毒操作。



图121

6.4.2 远程设置

通过瑞星管理员管理控制台的【全部】或【查毒】按钮，管理员可以对全部机器或指定的机器进行【分发查杀策略】以及【设置口令】的操作。使得管理员只需在管理控制台就可对所有用户的设置进行统一的管理和设定。为了避免人为的关闭或卸载客户端程序，管理控制台还提供了【设置口令】的功能。在口令的保护下，任何客户端都无法进行关闭实时监控和卸载程序的操作。

◆ 策略的分发

A）单击管理员管理控制台上的【全部】按钮或者选择【工具】/【对所有机器进行远程查杀毒】，弹出瑞星杀毒软件中小企业版远程查杀毒对话框。（如图122）



图122

B）单击【设置】菜单,选择【选项】进入设置界面,完成设置后点击确定，策略便被分发到所有的客户端机器中。具体各设置项的设置方法见下描述。（如图 123）

1、查杀设置：

点击【选项】后到默认的【杀毒设置】的界面。

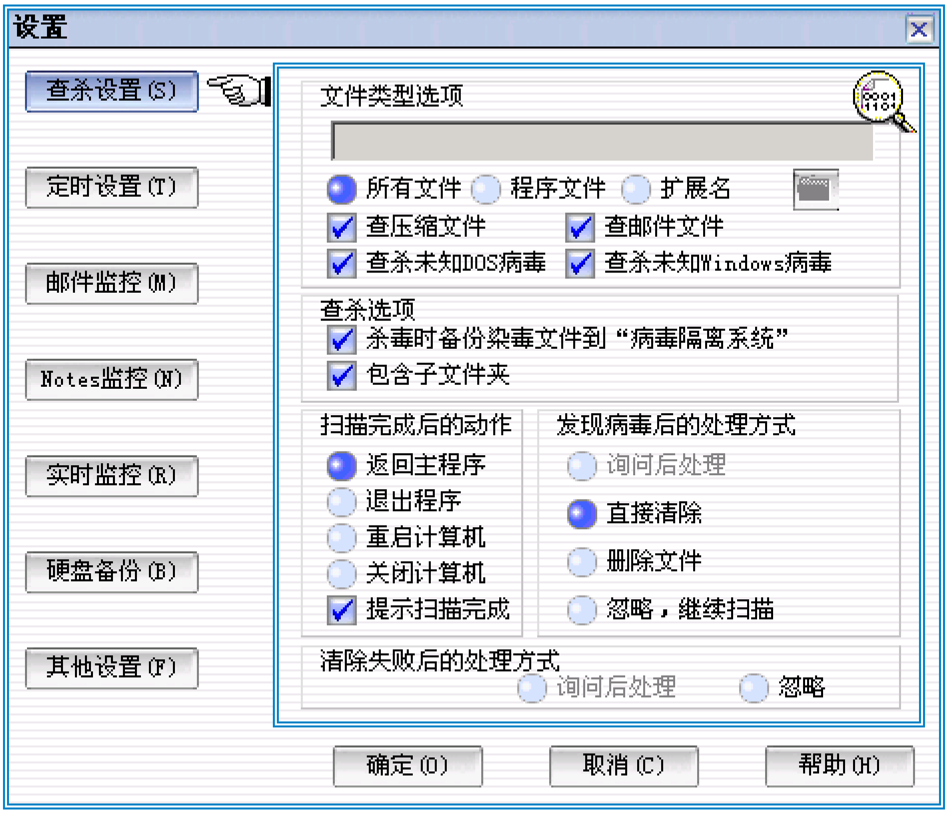


图 123

（1）文件类型选项

您可以通过对文件类型的选择确定要查杀的目标文件的类型。

【所有文件】项：选择后将监控任何格式的文件。

【程序文件】项：选择后将监测EXE、COM、SYS、VXD、DRV、DLL、BIN、OVL、386、SRC、HTM、HTML、FON、VBS、DOC、DOT、XLS、XLT等扩展名的文件。

【扩展名】项：选择后可以在提供的输入栏中输入需要的文件类型的扩展名，或者点击按钮在弹出的对话框中（如图124）根据自己的需要进行相应的文件类型的选择。

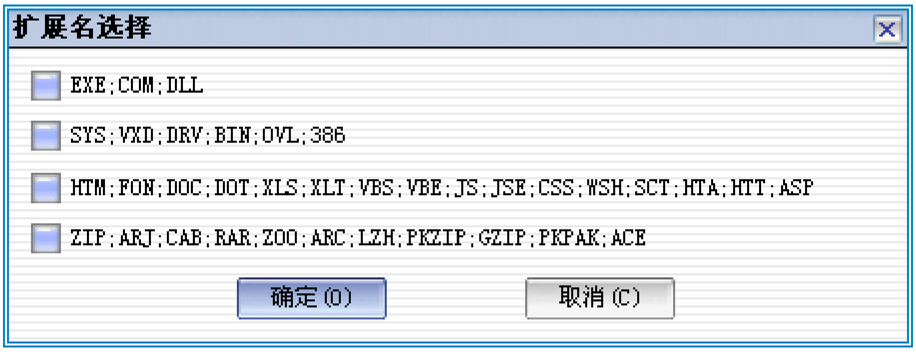


图124

【查压缩文件】：此选项被选中将查杀ZIP、ARJ、CAB、ZOO、RAR、ARC、LZH、GZIP等扩展名的压缩或自解压文件。

【查邮件文件】：选择后可以查杀所有识别的邮箱和邮件文件。

【查杀DOS病毒】：此选项被选中后可检测出携带未知的DOS病毒，您可以直接进行查杀处理或把可

以的文件发给瑞星公司进行分析。

【查未知Windows病毒】：此选项被选择后可检测出携带未知Windows病毒的文件，包括未知宏病毒和脚本病毒等。

（2）查杀选项

【备份染毒文件】：此项选中后在杀毒前,将会把所有您清除或删除的染毒文件备份在【病毒隔离系统】中隔离起来，如果您认为备份到病毒隔离系统中的染毒文件还有其它用途，可以从病毒隔离系统中将其恢复。

【包含子文件夹】：此选项被选择后将检测子文件夹中的文件是否带有病毒；如果不选，将只查杀指定的当前目录。

（3）扫描完成后的动作

【返回主程序】：此选项被选择后，杀毒动作完成后将自动返回到瑞星主程序。

【退出程序】：此选项被选择后，杀毒动作完成后将自动退出瑞星主程序。

【重启计算机】：此选项被选择后，杀毒动作完成后将自动重新启动计算机。

【关闭计算机】：此选项被选择后，杀毒动作完成后将自动关闭计算机。

【提示扫描完成】：为了方便查看和明确查杀结果，您选中该选项后，扫描完成时会出现本次查杀病毒具体信息的提示。（建议用户选择 【提示扫描完成】的方式）

（4）发现病毒后的处理方式

【询问后处理】：此选项被选择后，查毒过程中发现病毒将询问用户如何处理（建议用户使用【询问后处理】的方式）。

【直接清除】：此选项被选择后，查毒过程中发现病毒后将直接清除。

【删除文件】：此选项被选择后，查毒过程中发现病毒后将直接删除带毒文件。

【忽略，继续扫描】：此选项被选择后，查毒过程中发现病毒将不作任何处理继续进行扫描。

（5）清除失败后的处理方式

清除失败后可选择 【询问后处理】和【忽略】两种方式，进一步保证即不漏过也不错杀可疑文件。

以上设置结束后，点击】确定【按钮，即可生效。如需返回缺省设置，请选择【设置】菜单中的「恢复缺省设置」命令即可。

2、【定时设置】项：

点击【选项】进入【定时设置】的界面（如图 125）

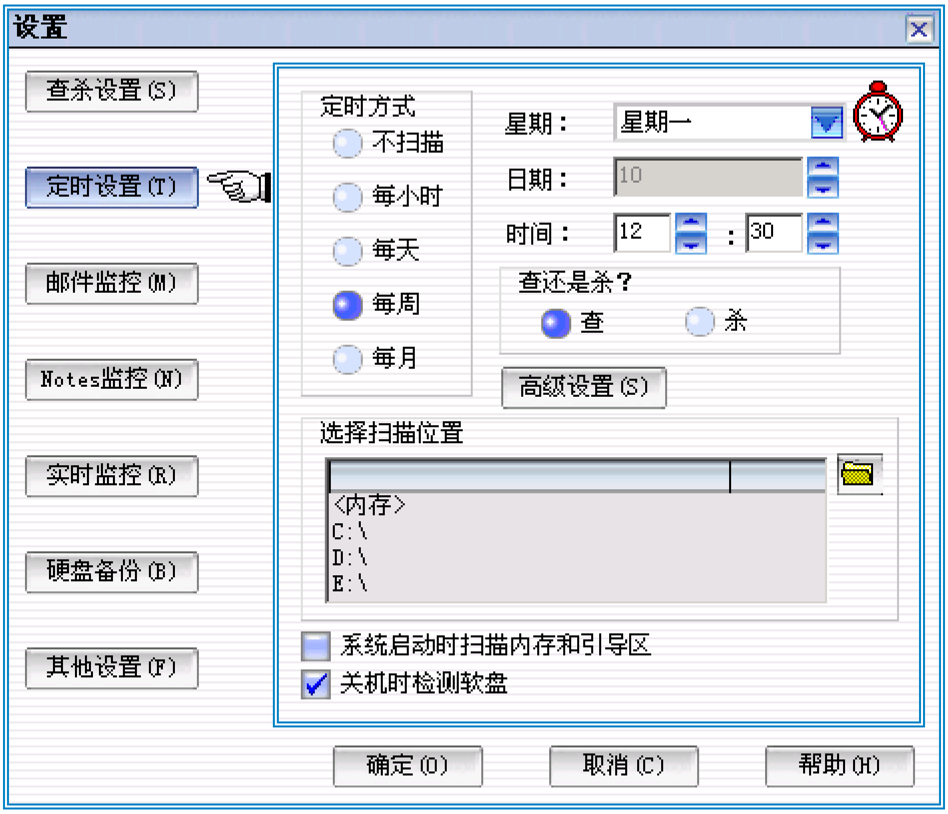


图 125

根据不同的需要，不同的用户可以在定时查杀病毒设置页面选定自己希望瑞星杀毒软件【网络版】对自己的计算机进行定时查杀的时间，可在时间设置内分别选择【不扫描】、【每小时】、【每日】、【每周】、【每月】等不同扫描频率；（如每小时 10 分钟或每日 10：00 或每周，星期一，12：00 或每月，10 日，10：00）。

【高级设置】：您还可以根据自己对计算机掌握程度的不同来决定是否进入【定时查杀高级设置】选项来进一步详细的设置您的定时查杀功能。

【系统启动时扫描内存和引导区】：此项功能选择后，每次系统启动进入时将会扫描内存和引导区，以保证您有干净的系统环境来开始工作。

【关机时检测软盘】：此项功能选择后，每次系统关闭时会检查软区里的软盘是否带毒，防止下次系统启动时感染引导型病毒。

3、【邮件监控】项：

点击【选项】进入【邮件监控】的界面（如图 126）

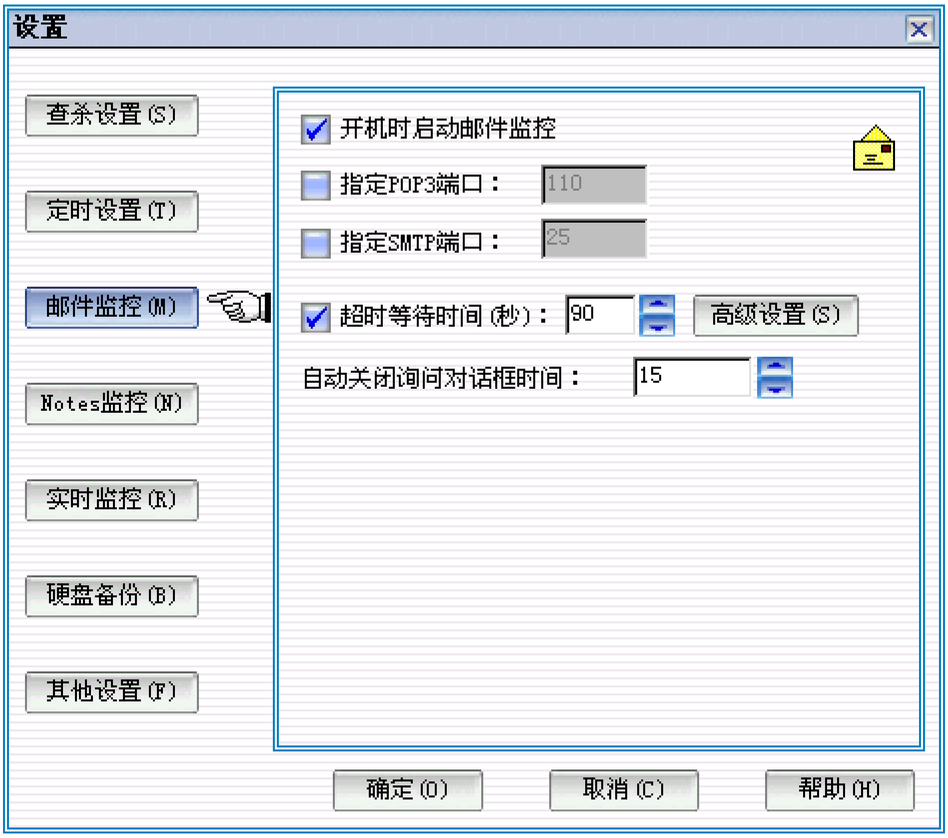


图 126

邮件监控是“瑞星杀毒软件”新增功能，当您使用 Microsoft Outlook 或 Outlook Express 接收、发送和阅览电子邮件时，如果邮件附件染毒，邮件监控会立即提醒您并提供多种方式对含染毒附件进行处理。（具体使用方法和设置请参阅 5.2）

4、【Notes 监控】项：

点击【选项】进入【Notes 监控】的界面（如图 127）

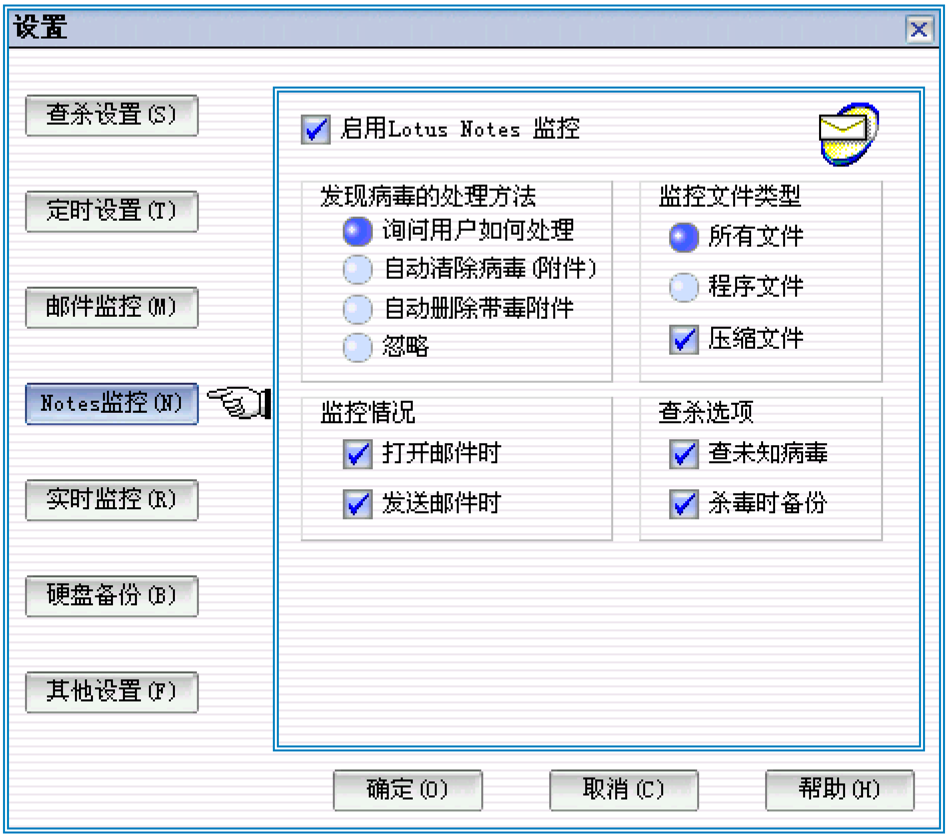


图 127

如果您安装了 Lotus Notes,可以通过【Notes 监控】对 Lotus Notes 邮件监控进行设置（使用方法和设置请参阅 5.3），Notes 邮件监控是可选组件，典型安装中会自动安装在您的机器中，您也可在自定义安装中进行选择。

提示：对 Lotus Notes 邮件监控设置更改后，需要重新启动 Lotus Notes 设置才能生效。

5、菜单【实时监控】项 ：

点击【选项】进入【实时监控】的界面（如图 128）（实时监控使用方法和设置请参阅 5.1）

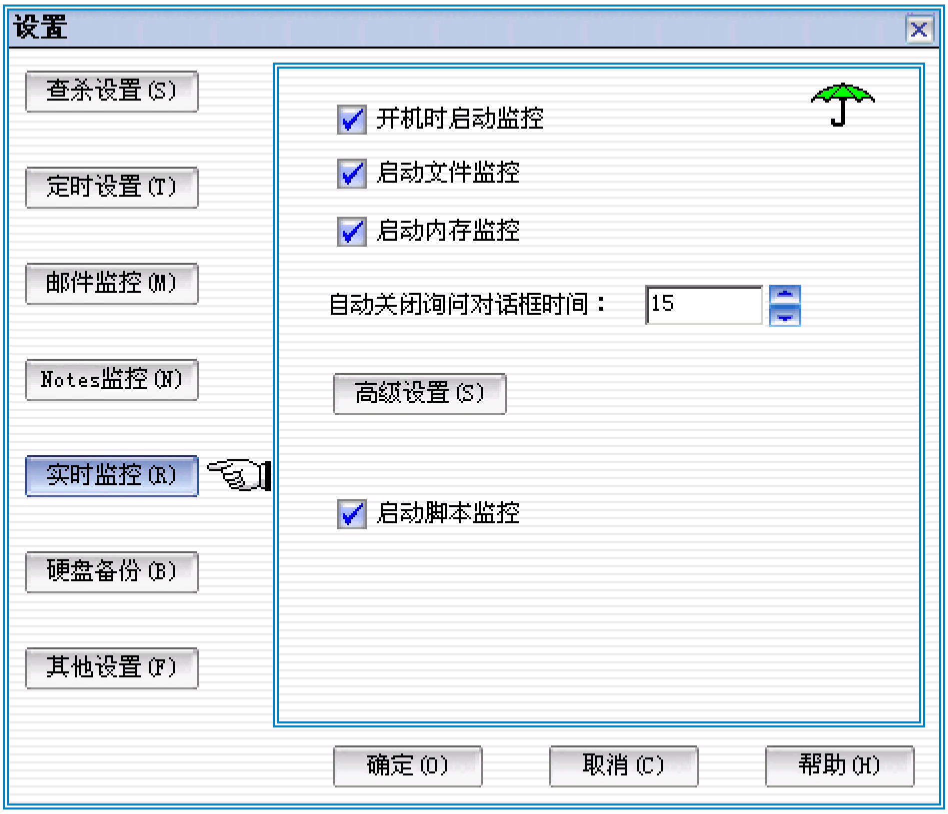


图 128

6、【病毒报警】项：

点击【选项】进入【病毒报警】的界面（如图 129）

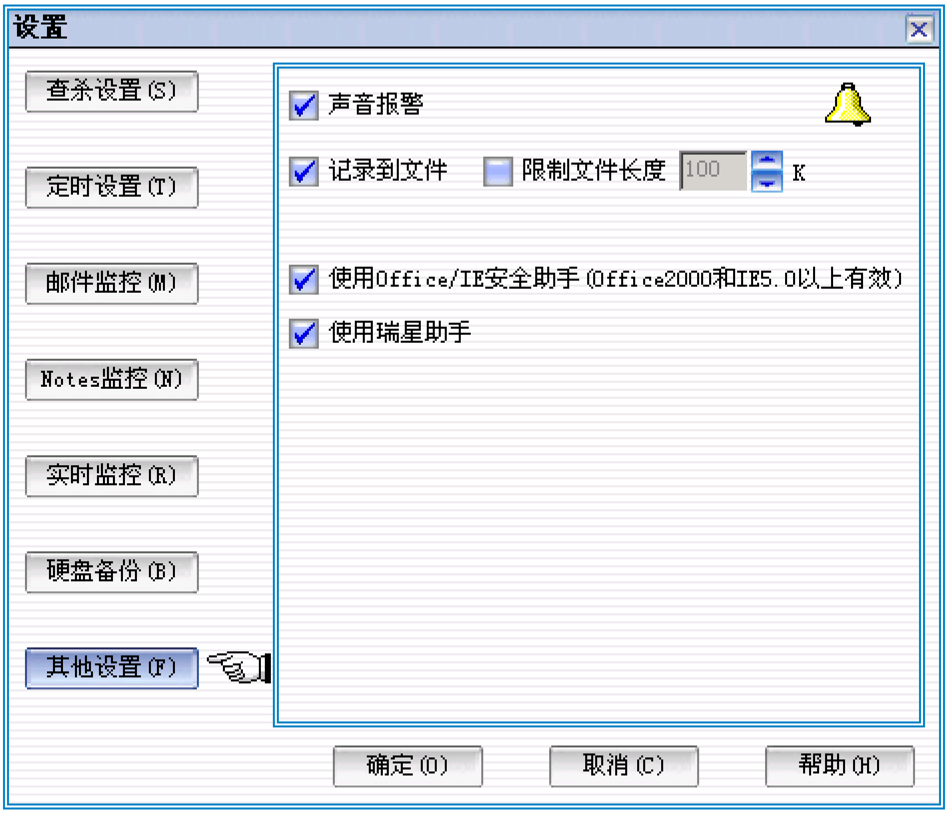


图 129

【声音报警】：此项功能选择后，在检测到病毒时，瑞星软件将通过声卡或 PC 喇叭两种方式（由电脑配置自动选择）提醒您注意。如您不需要声音报警也可以关闭。

提示：如果希望加快杀毒速度，不建议选择此项设置。

【记录到文件】：此项功能选择后，您可以设置检测到病毒时是否写入历史记录，并限制历史记录文件的长度。

【使用 Office/IE 安全助手】：此项功能选择后，当您使用 Office2000 和 IE 的时候，瑞星的安全助手能提供保护功能。当该选项处未选状态时，瑞星安全助手不起作用。

注：该功能只在 Office2000 和 IE 5.0 以上时，才可以有效使用。

7、菜单【硬盘备份】项：

点击【选项】进入【硬盘备份】的界面（如图 130），您可以根据自身的需要制订富有个性的硬盘信息备份时间计划，以保障您的备份文件是最新的。（硬盘备份的具体使用见 4.2.2）

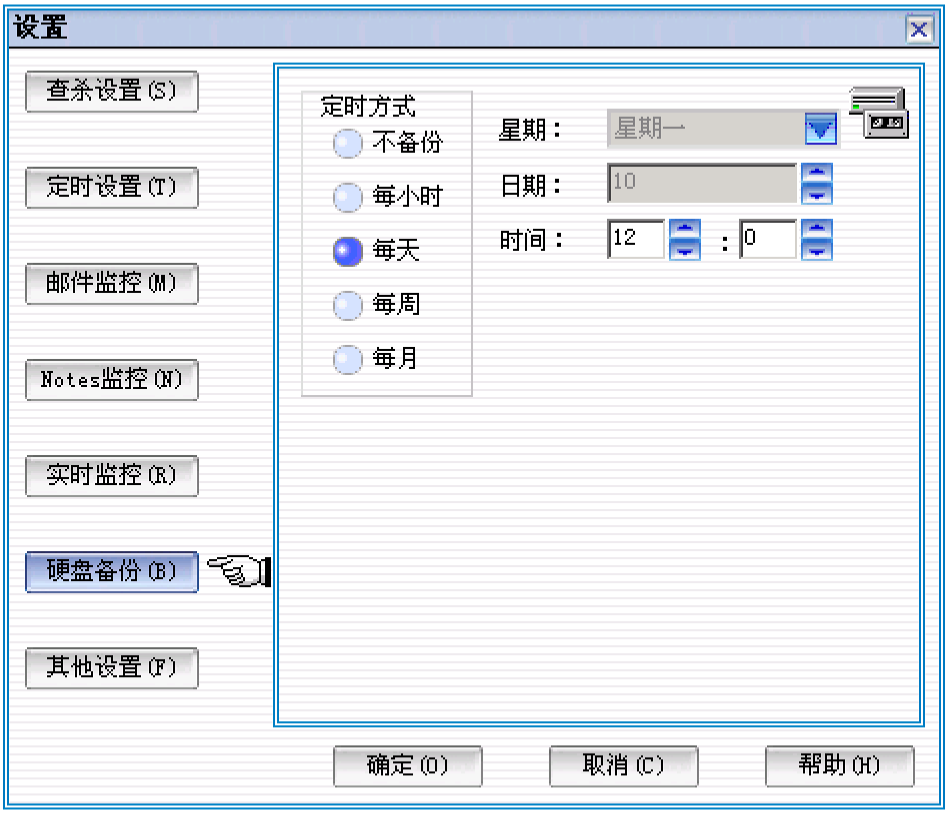


图 130

◆ 设置客户端口令

为了避免客户端用户人为的关闭实时监控程序或卸载杀毒程序，从而造成整体防毒体系的漏洞，管理员可以通过管理控制台程序为所有或指定的用户设置密码保护。

A)为指定的用户添加口令

在【计算机列表栏】选中需设定密码的用户，单击鼠标右键选择【设置客户端口令】（如图131）

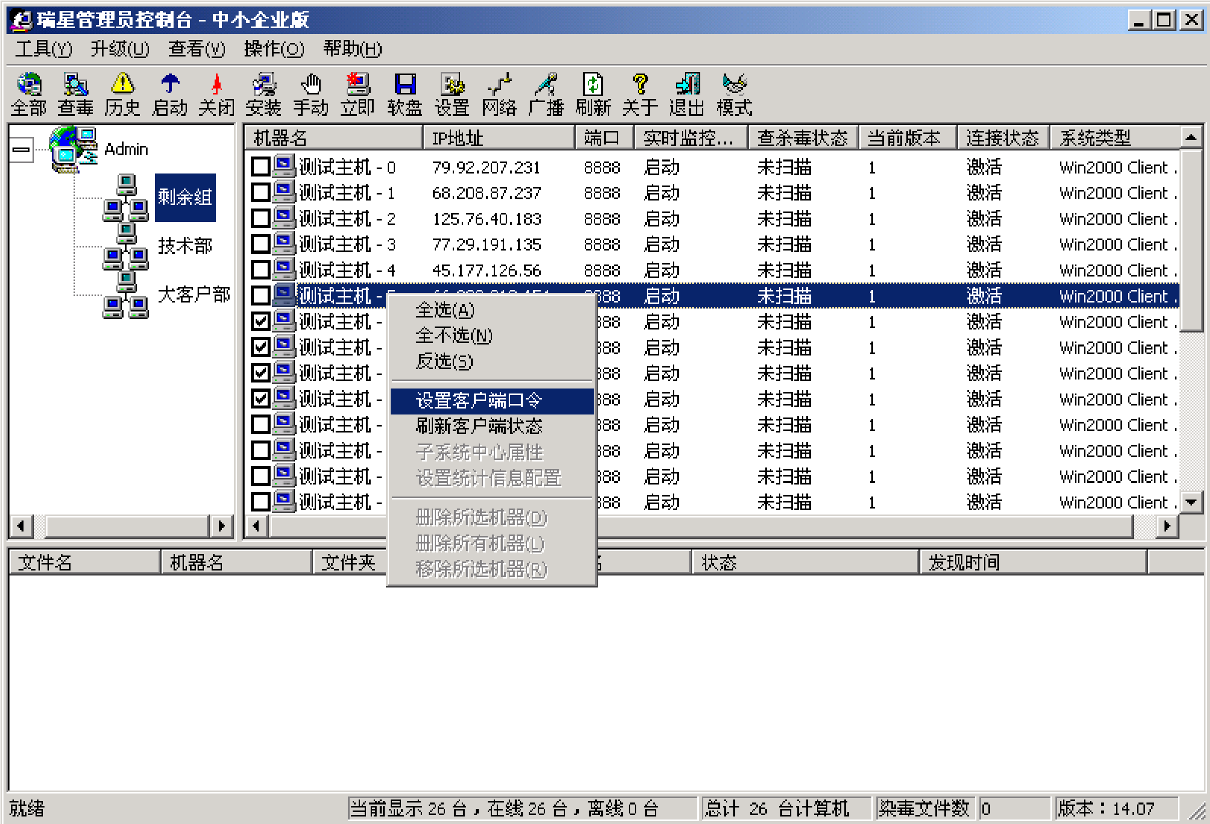


图131

第一步：在弹出的对话框中，输入密码按确定后密码生效（如图132）



图132

第二步：密码设置完成后，客户端将在卸载杀毒程序或关闭实时监控将出现【请输入密码】的提示框。（如图133）



图133

B)为组添加密码

如果您想为不同的用户组设定不同的组密码，您可以在【组管理栏】里选中该组，单击鼠标右键选定【设置组密码】。（如图134）

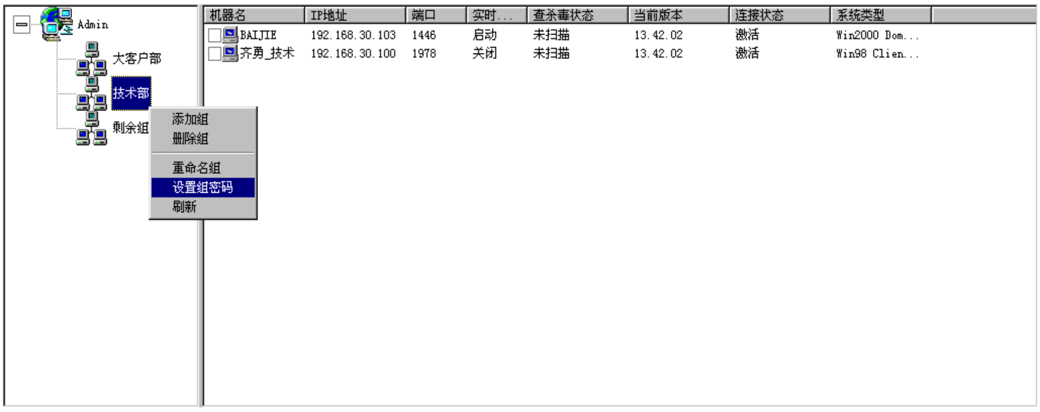


图134

在弹出的【设置客户端口令】对话框中输入密码按确定后密码生效。（如图135）



图135

提示:以上所有的远程设置功能，仅对处于激活状态的客户端有效。（关于组管理的更多信息详见6.5）

6.4.3 远程安装

通过瑞星管理员管理控制台不仅可以为局域网上的所有客户端安装管理控制台也可以为基于NT结构的操作系统远程安装瑞星杀毒软件， 远程安装功能极大的方便了系统管理员的管理和安装工作。

◆ 远程安装管理员管理控制台

瑞星杀毒软件中小企业版系统管理员可以将【瑞星管理员管理控制台】安装到他认为合适的计算机上。安装方法如下：

A)在【计算机列表栏】选中您认为合适的机器，单击【工具】菜单，选中【远程安装管理员管理控制台】或按工具栏【安装】快捷图标，即可在选中的计算机上进行【瑞星管理员管理控制台】的远程安装；（如图136）

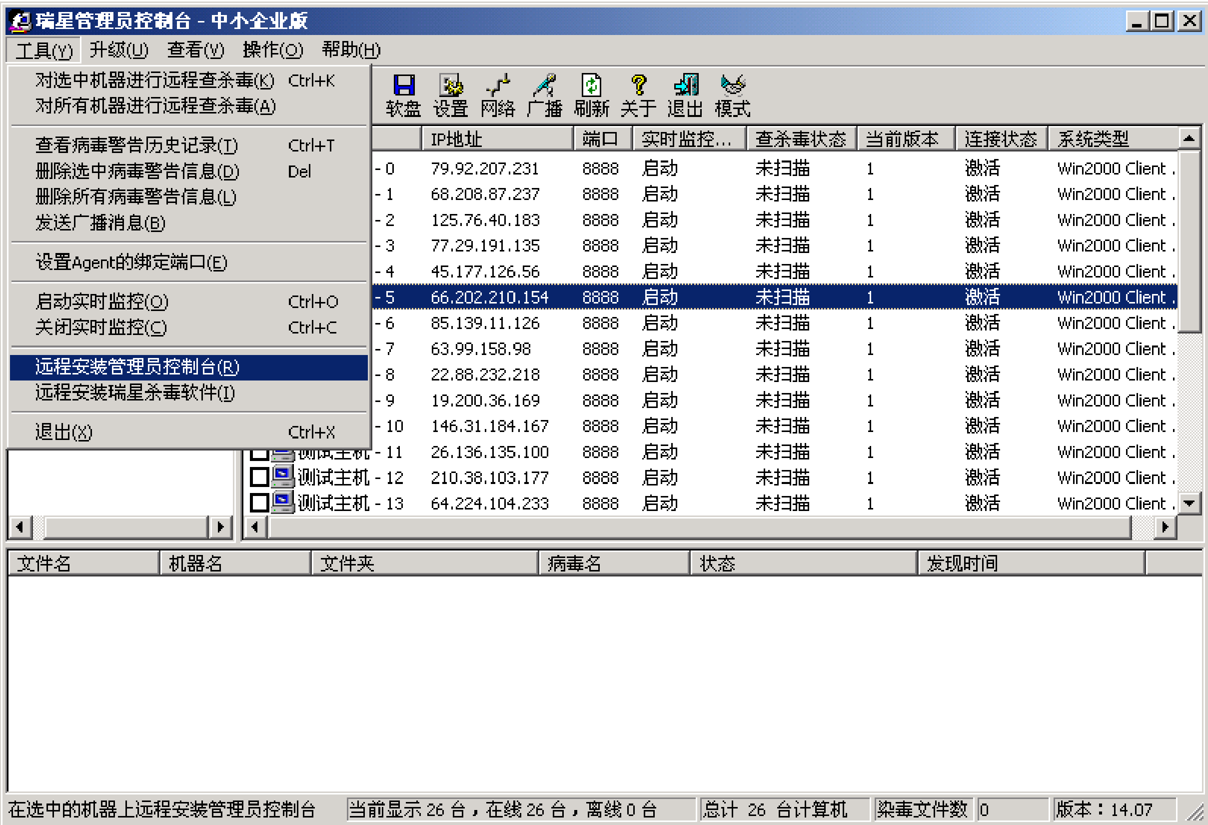


图136

B)单击 ‘远程安装管理员管理控制台’菜单项，在弹出的提示对话框，选择【确定】按钮（如图137）



图137

C)安装完成后，本机给出提示，单击确定完成管理控制台的安装。（如图138）



图138

查看目标机器的安装情况，您可以看见桌面上出现了【】图标。

提示：建议不要在局域网上安装过多的管理控制台以保障管理的统一。

◆ 远程安装瑞星杀毒软件

瑞星杀毒软件中小企业版系统管理员可以通过瑞星管理控制台程序给指定的基于NT系统的网络用户进行远程安装瑞星杀毒软件的操作。

安装方法如下：

A)单击【工具】菜单栏，选择【远程安装瑞星杀毒软件】（如图139）

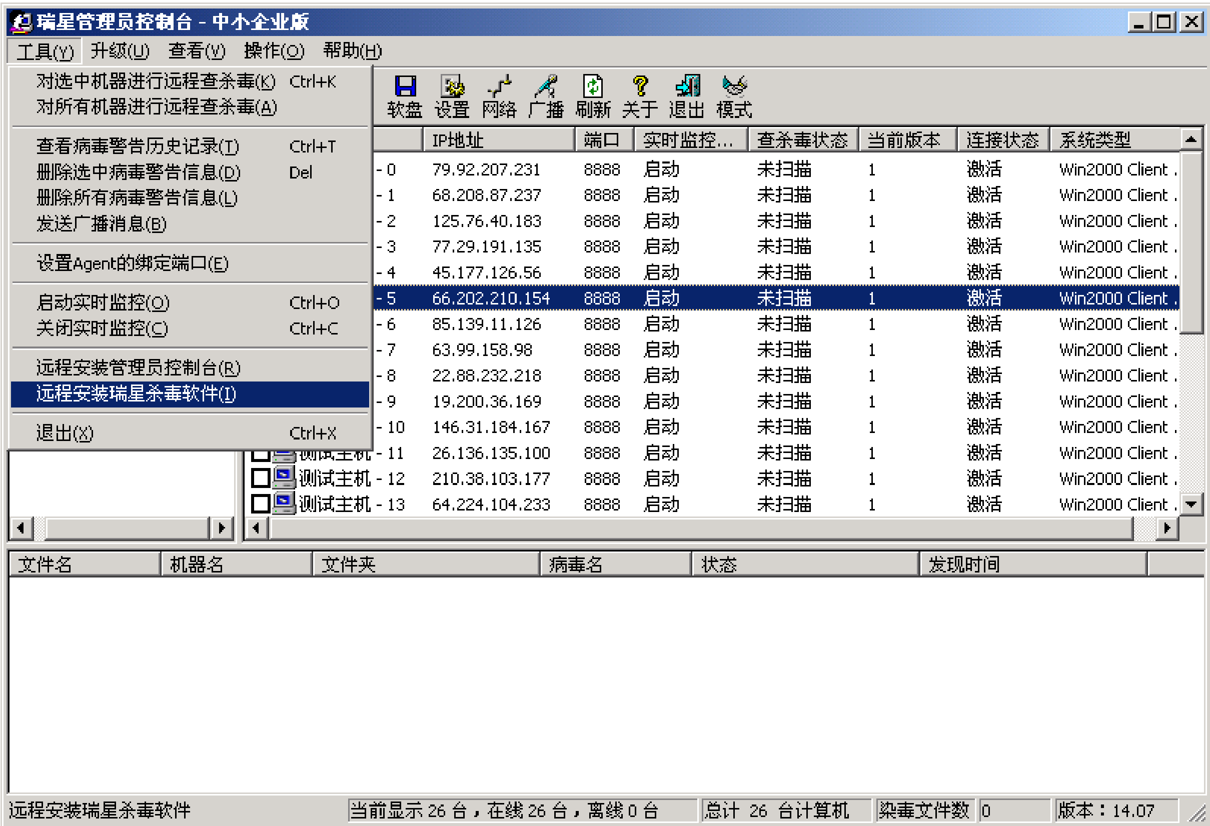


图139

B)在弹出的对话框中选中您需要安装瑞星杀毒软件的机器，单击【添加】按钮。（如图140）

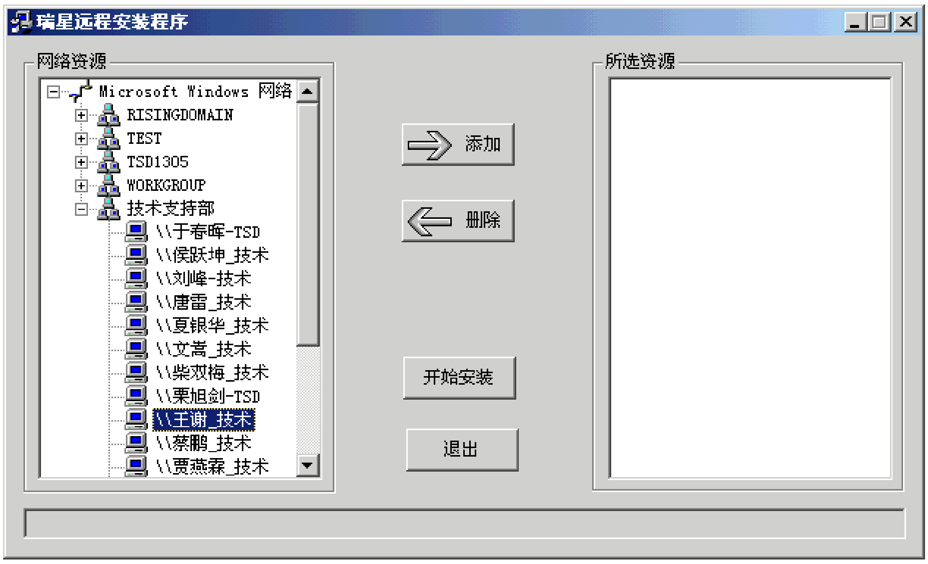


图140

C)在弹出的【输入\\ 管理员密码】的提示框中，输入目标机的管理员密码，单击确定。（如图141）

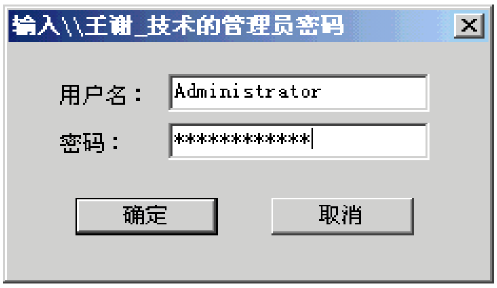


图141

D)目标计算机被添加到【所选资源】框中后，单击【开始安装】按钮，可以看见【安装状态栏】显示正在为目标机器安装的提示信息。（如图142）



图142

E)安装完成后，在【安装状态栏】显示【安装完成!】的提示（如图143）



图143

F)被远程安装瑞星杀毒软件的用户桌面将出现【信使服务】的提示框，单击确定。远程安装完成。（如图144）



图144

注意：因操作系统局限，针对Windows 9x/me/xp系统的客户端，管理控制台的【远程安装杀毒软件】功能不能实现。

6.4.4 远程启动

管理员通过瑞星管理控制台程序可以实时地查看目前所有客户端的情况，包括是否启动或关闭了瑞星实时监控程序。同时也可以通过按工具栏的【启动】和【关闭】按钮来远程控制客户端的监控状态。（如图145）

机器名	IP地址	端口	实时监控...	查杀毒状态	当前版本	连接状态	系统类型
☐ 测试主机 - 12	210.38.103.177	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 13	64.224.104.233	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 14	215.63.21.61	8888	启动	未扫描	1	激活	Win2000 Client .
☑ 测试主机 - 15	24.101.85.200	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 16	201.186.21.182	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 17	29.58.96.70	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 18	60.250.21.241	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 19	11.248.214.117	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 20	165.160.100.27	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 21	99.46.16.237	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 22	228.94.86.61	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 23	254.127.108.36	8888	启动	未扫描	1	激活	Win2000 Client .
☐ TEST7	192.168.0.3	1775	关闭	未扫描	14.07	激活	Win2000 Domai.
☑ WANGXIULIANG	192.168.0.1	1026	关闭	未扫描	14.08	激活	WinMe Client ...

图145

- ◆ 选中【实时监控】 状态处于关闭的机器，选择【工具】/【启动实时监控】或单击工具栏【启动】按钮，即可为选中的计算机开启监控系统。（如图146）

机器名	IP地址	端口	实时监控...	查杀毒状态	当前版本	连接状态	系统类型
☐ 测试主机 - 12	210.38.103.177	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 13	64.224.104.233	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 14	215.63.21.61	8888	启动	未扫描	1	激活	Win2000 Client .
☑ 测试主机 - 15	24.101.85.200	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 16	201.186.21.182	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 17	29.58.96.70	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 18	60.250.21.241	8888	启动	未扫描	1	激活	Win2000 Client .
☐ 测试主机 - 19	11.248.214.117	8888	启动	未扫描	1	激活	Win2000 Client .

图146

◆ 选中处于启动实时监控状态的机器，选择【工具】/【关闭实时监控】或单击工具栏【关闭】按钮，即可完成对选中计算机关闭监控的操作。

注意：如果您选定的客户端处于“未激活”状态，那么该远程启动命令是无效的。

6.4.5 远程报警

全网中瑞星杀毒软件发现的任何病毒信息和对病毒的处理方法的相关信息都将传递到系统中心，并在管理控制台的【病毒信息列表栏】中显示。管理员可以通过该功能方便的了解全网的安全状况，并可根据具体情况做出适当的处理。（如图147）

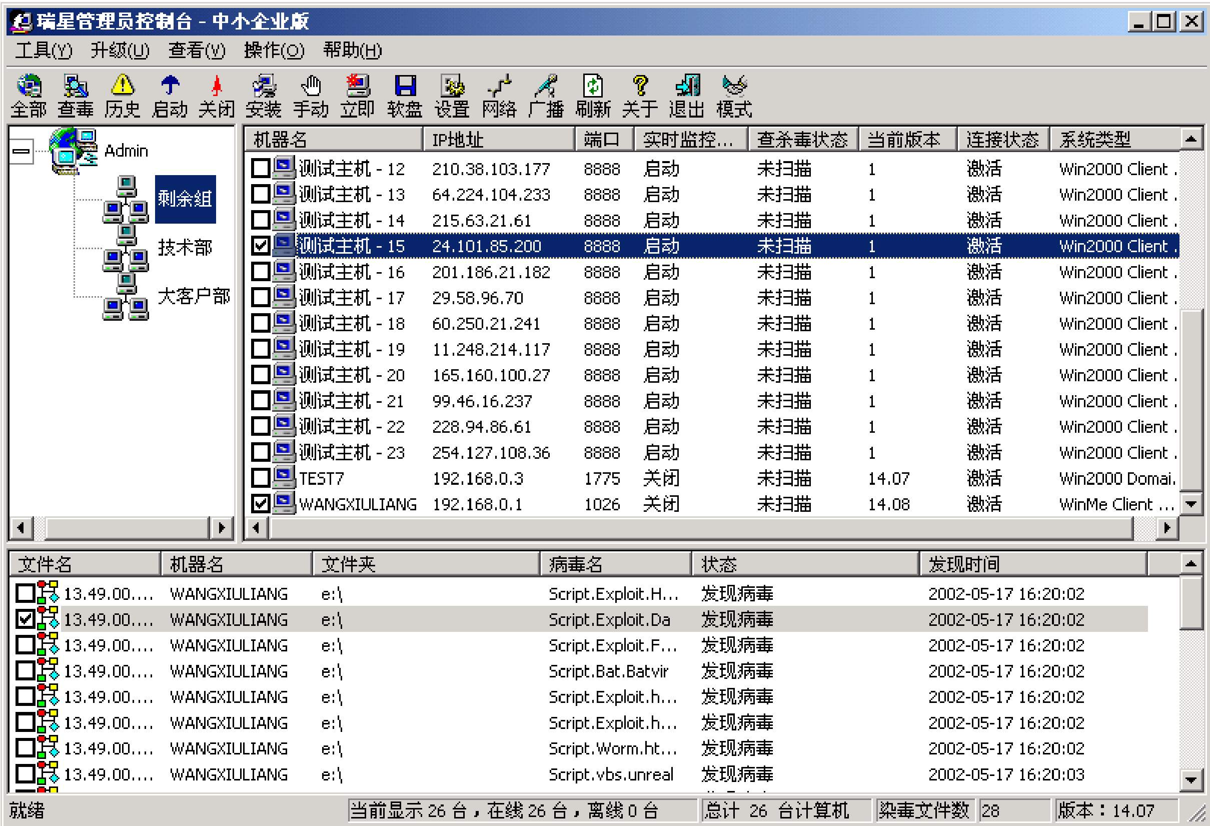


图147

6.4.6 远程全网查杀

‘远程全网查杀毒’是网络版杀毒软件整体保护网络安全的重要功能。远程全网查杀毒的特点在于‘整体性’和‘实时性’。即，其查杀的范围是网络中所有安装了瑞星网络版杀毒软件的计算机。查杀毒利用客户端本地的杀毒程序，个个客户端查杀毒没有先后顺序而是同时启动。这样，就保障了所有客户端的计算机几乎在同一时刻进行杀毒的工作，避免了病毒交叉感染。管理员可以通过管理控制台有计划的对网络上所有的计算机同时进行远程查杀毒操作。如果此时网络上有的计算机没有开机或处于“未激活”状态，那么只需要这些计算机是注册过的合法用户，当它们一旦启动，即会自动进行查杀病毒的工作。

进入瑞星管理员管理控制台后，单击【工具】菜单栏，选择【对所有机器进行远程查杀毒】(如图148)。

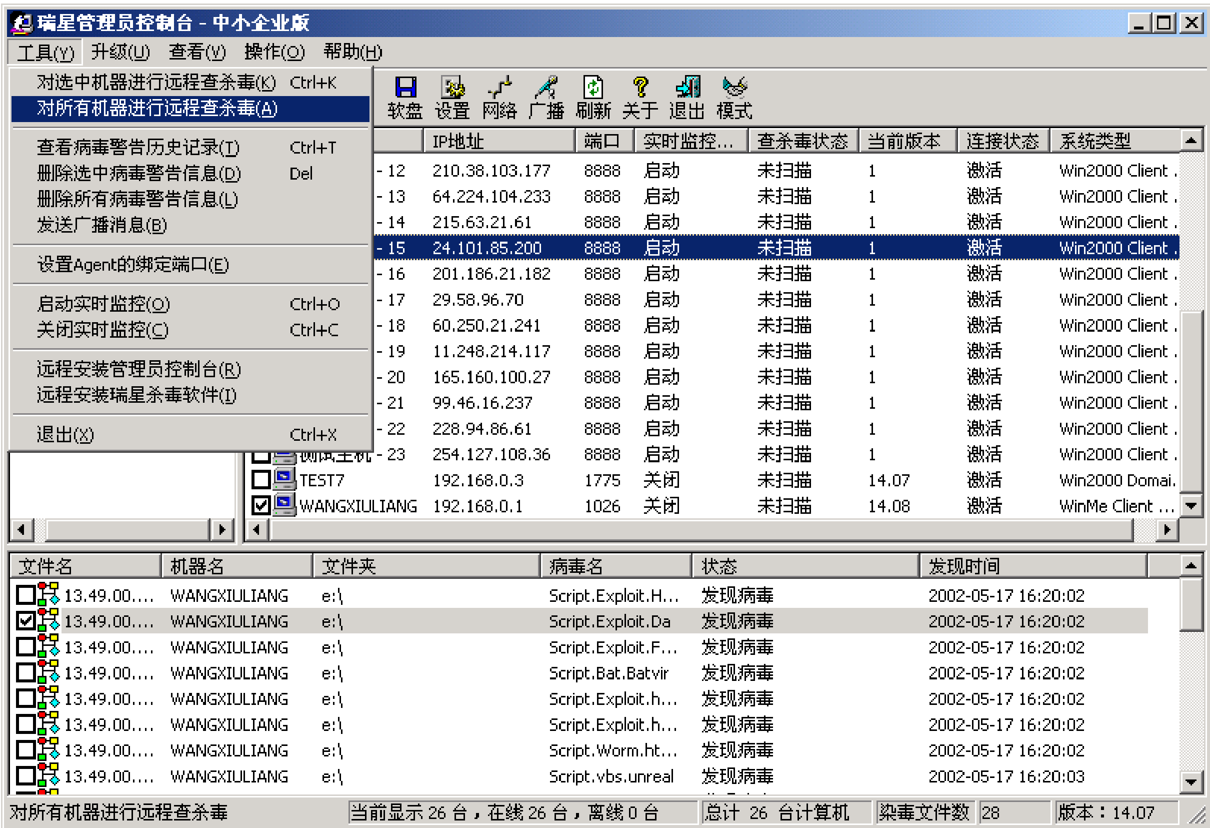


图148

在弹出的“瑞星杀毒软件中小企业版（所有机器）”程序界面中单击【杀毒】按钮。(如图149)



图149

在该程序界面的底部，看以查看当前的查杀文件数及感染病毒的文件总数。(如图150)

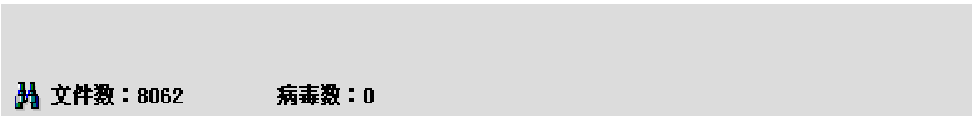


图150

在“瑞星杀毒软件【网络版】（所有机器）”程序界面中单击【停止】即可停止远程全网查杀的工作。

6.5 用户管理

控制管理作为瑞星杀毒软件（网络版）的一个管理特色，其核心在于在一个管理控制台中可以进行多模式管理。即组的管理模式与管理员的多级管理模式。在管理控制台中，只要通过【模式】的按钮就可以在两个不同的管理模式中灵活切换，使得管理员能够轻松的在一个界面中实现多层次多级的管理。

6.5.1 组管理模式

◆ 启动：启动管理员管理控制台后，默认进入到组管理模式中。

◆ 组管理模式的应用：

A)建立组

方法一：

1、以 ADMIN 身份登录进入组管理模式。

2、用鼠标右键点击【Admin】进入（如图 151）的界面

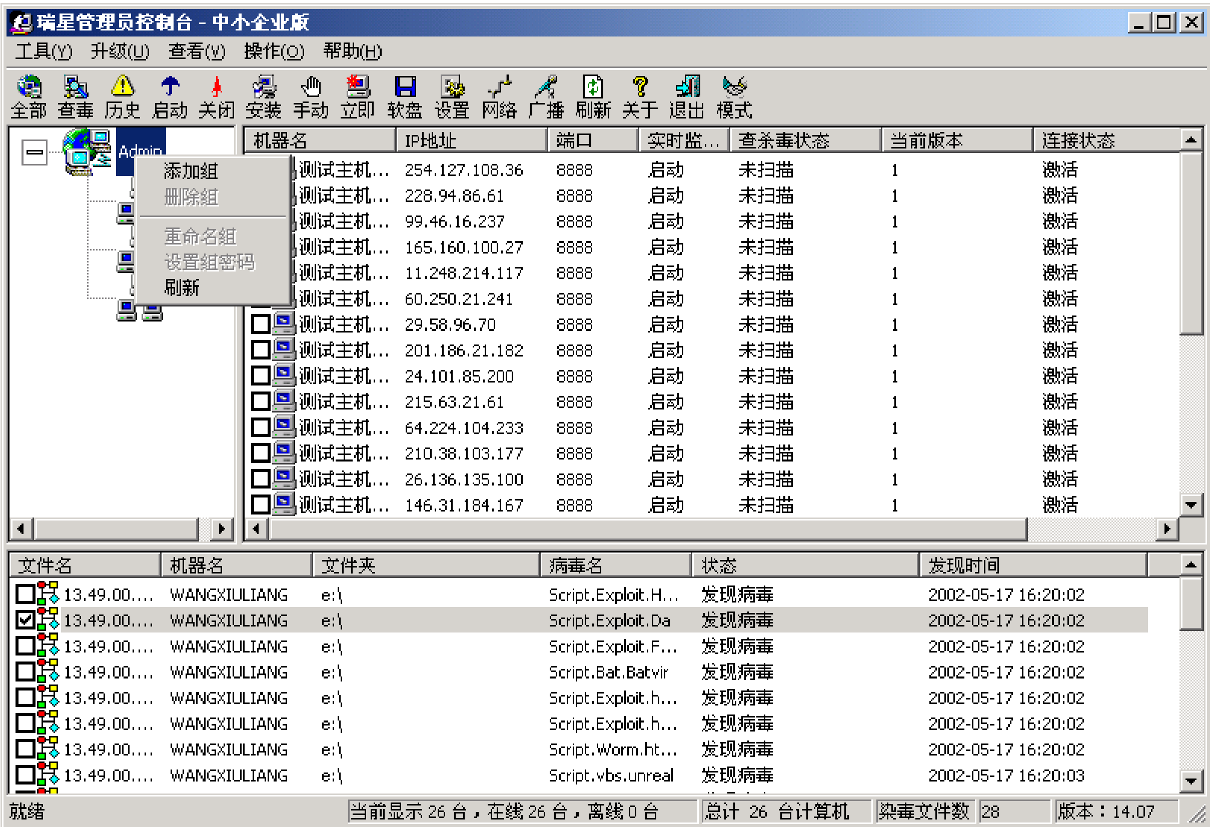


图 151

3、单击‘添加组’添加新的管理组。

注意：新建立组的名称为“New Group”，可以选中该组后重新命名。

方法二：

1、以 ADMIN 身份登录进入组管理模式。

2、选择菜单【操作】选中【添加组】项。(如图 152)

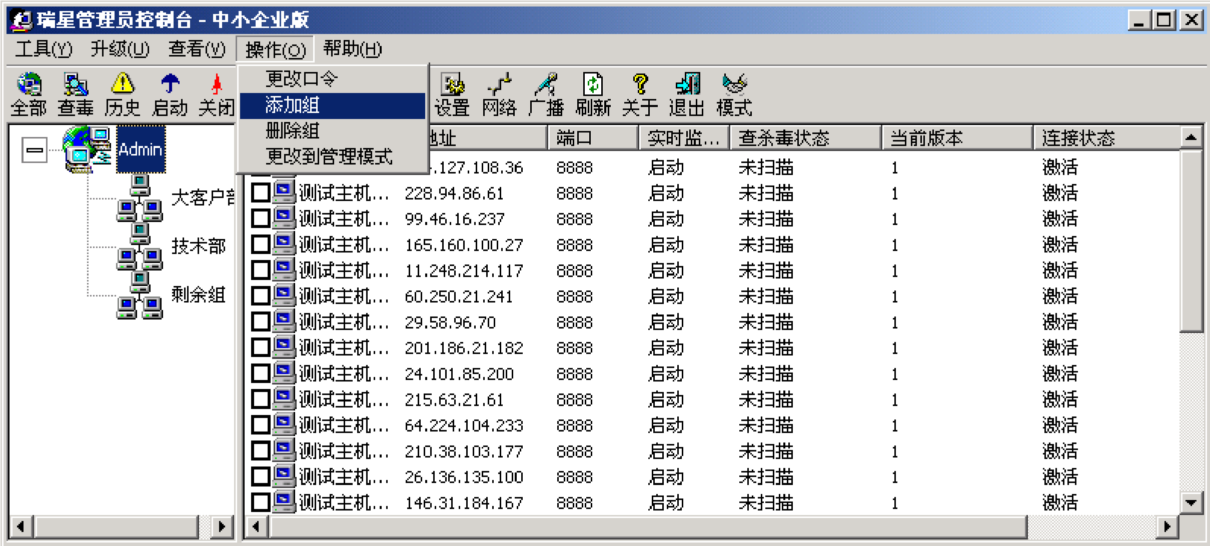


图 152

B)为指定的组添加用户

1、以 ADMIN 身份登录进入组管理模式。

2、鼠标单击【剩余组】，使【剩余组】被选中。(如图 153)

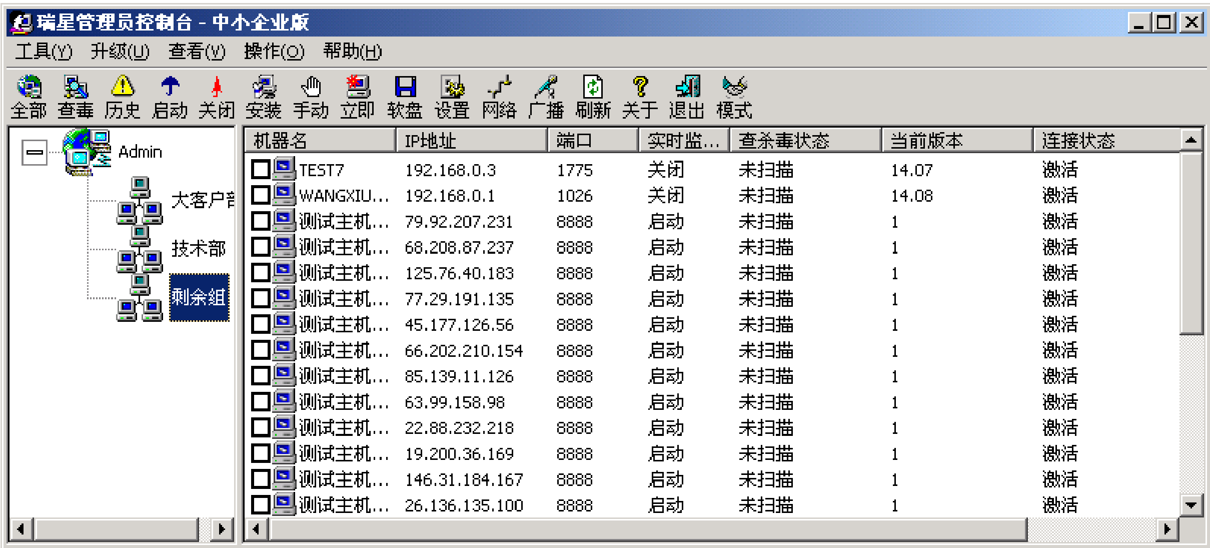


图 153

3、选中希望加入指定组的计算机。(如图 154)

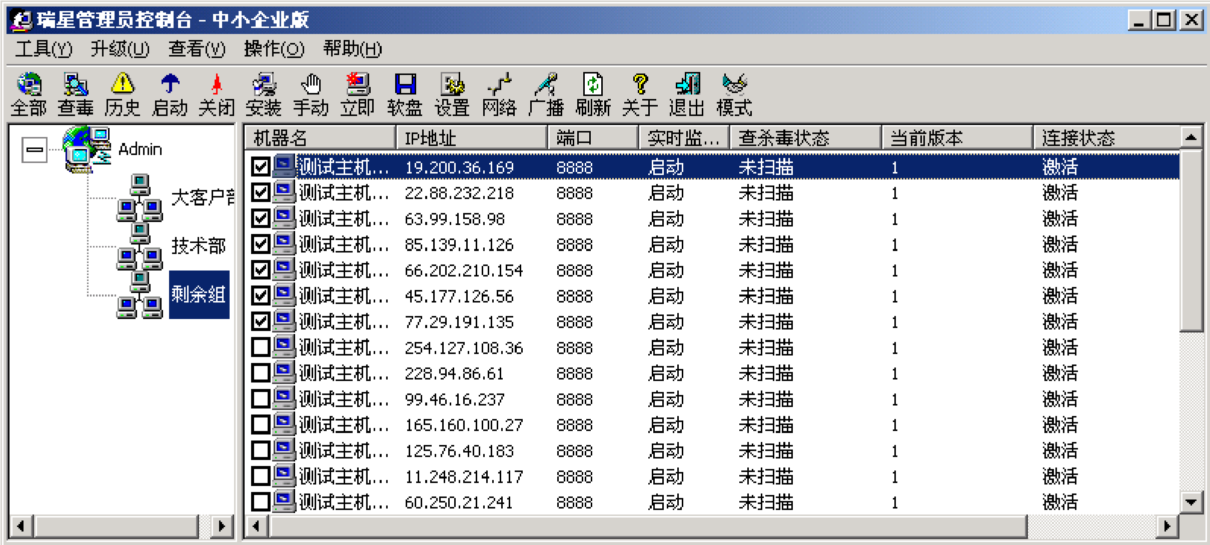


图 154

4、选中的计算机用鼠标‘拖进’指定的组中。（如图 155）

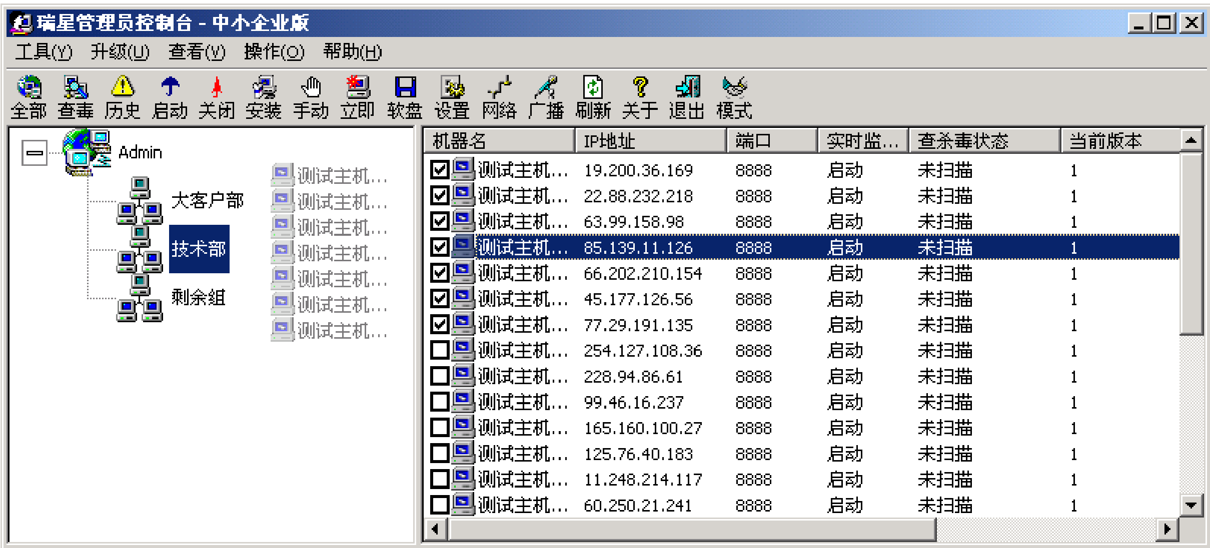


图 155

5、组用户添加完成。（如图 156）

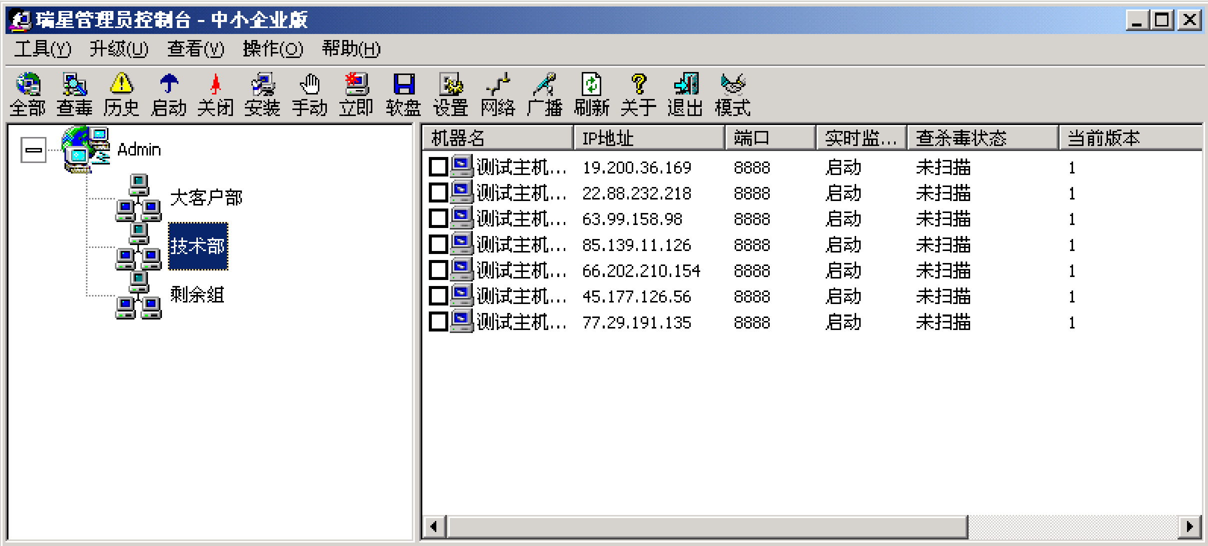


图 156

C)删除组

方法一、选定希望删除的组，点击鼠标右键点击‘删除’。(如图 157）

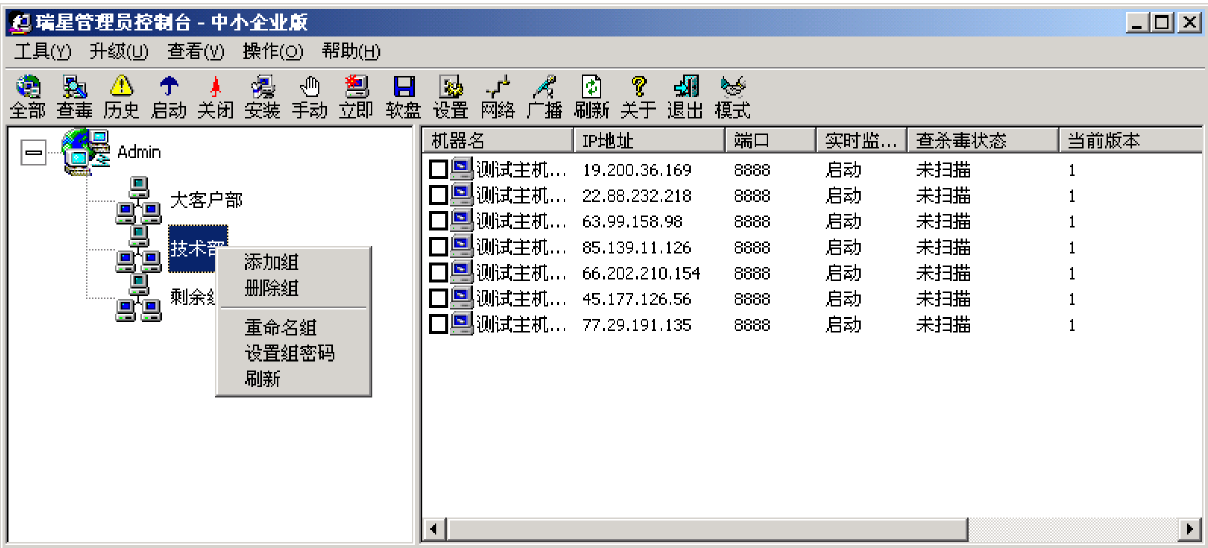


图 157

方法二、选定希望删除的组，点击菜单【操作】中的【删除组】项。(如图 158）

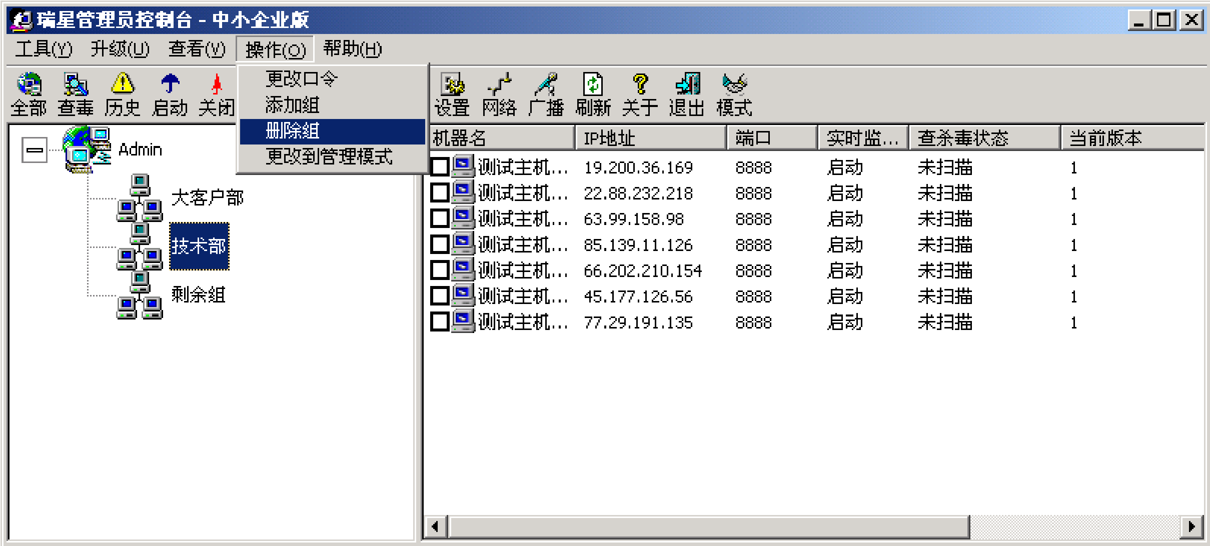


图 158

6.5.2 管理员管理模式

◆ 启动

通过 ADMIN 管理员账号登录到管理控制台，单击【模式】按钮或者单击【操作】菜单中的【更改到管理模式】即可进入管理员管理模式。（如图 159）

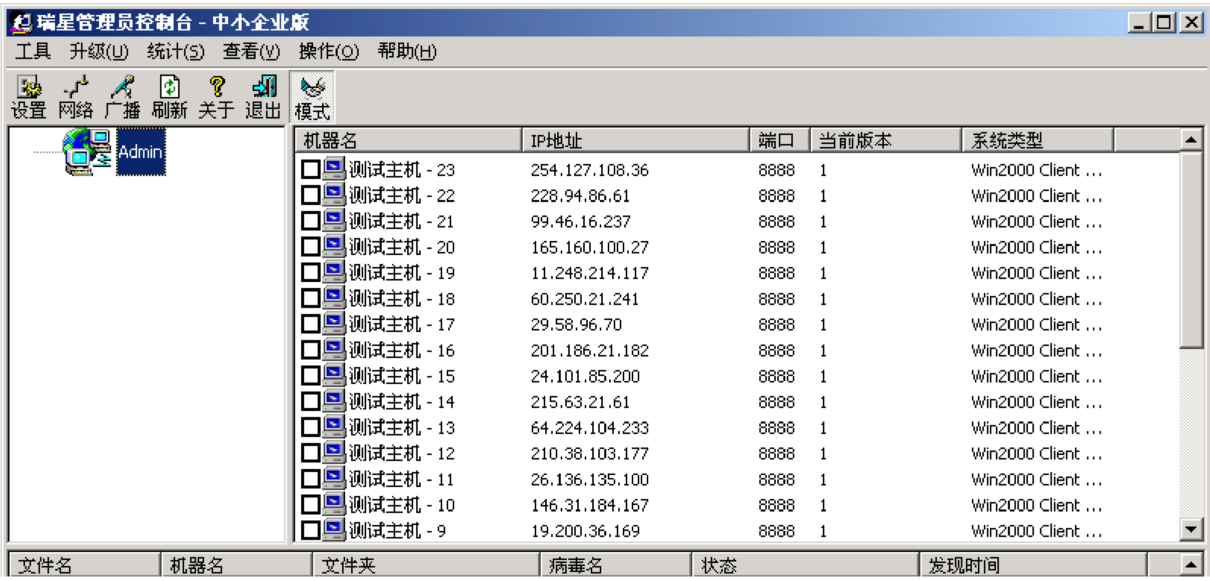


图 159

◆ 管理员管理模式的基本应用

A)建立管理员：

瑞星杀毒软件中小企业版支持两层用户管理即“ADMIN”超级用户的管理和通过“ADMIN”建立的普通管理员的管理。ADMIN 可以为普通管理员分配其管理的计算机，并为普通管理员设置密码。普通管理员可以通过 ADMIN 创建的账号名和密码登录进入管理控制台对特定的计算机进行管

理。

1、进入管理员管理模式；

2、在管理员管理区内点击鼠标右键点击【添加管理员】。（如图 160）



图 160

提示：也可以通过单击菜单【操作】中的【添加管理员项】添加新的管理员。

B)添加管理对象

1、为普通管理员分配管理对象。（如图 161）

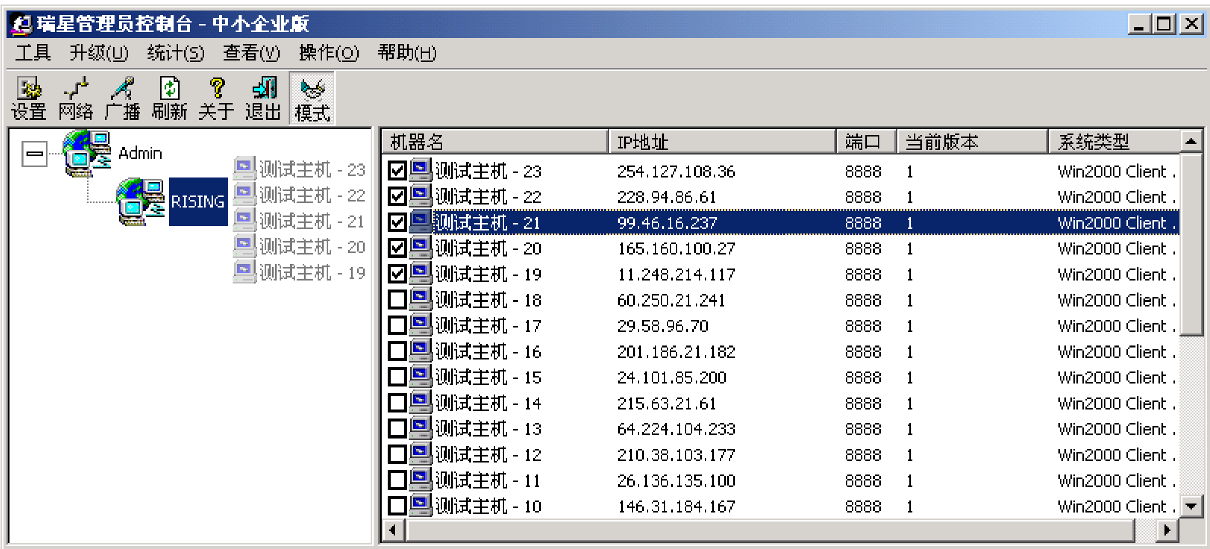


图 161

2、添加管理对象完成（如图 162）

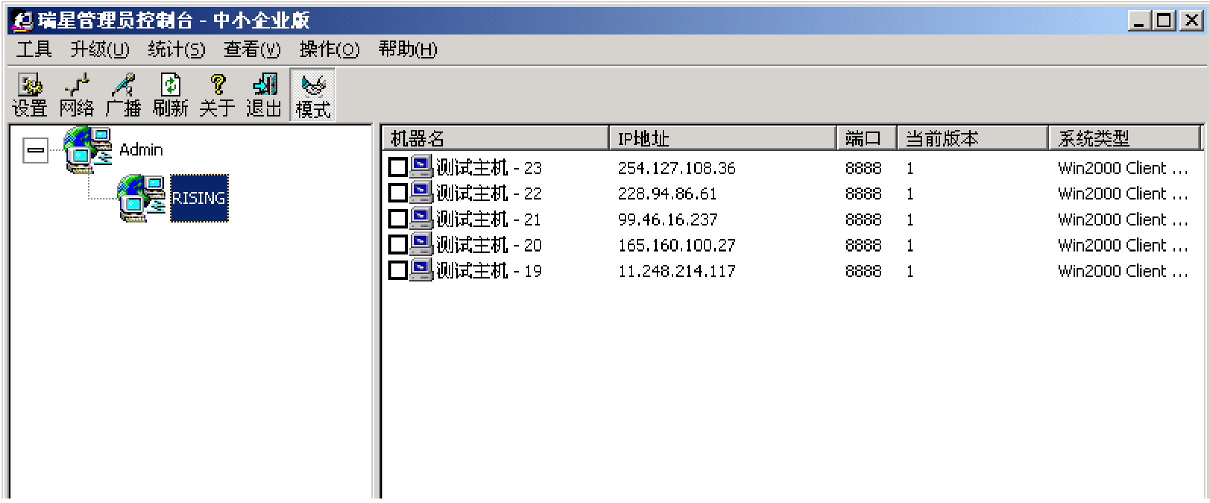


图 162

3、普通管理员登录（如图 163）



图 163

提示：普通管理员通过 ADMIN 创建的账号和密码登录。

C)删除管理员：

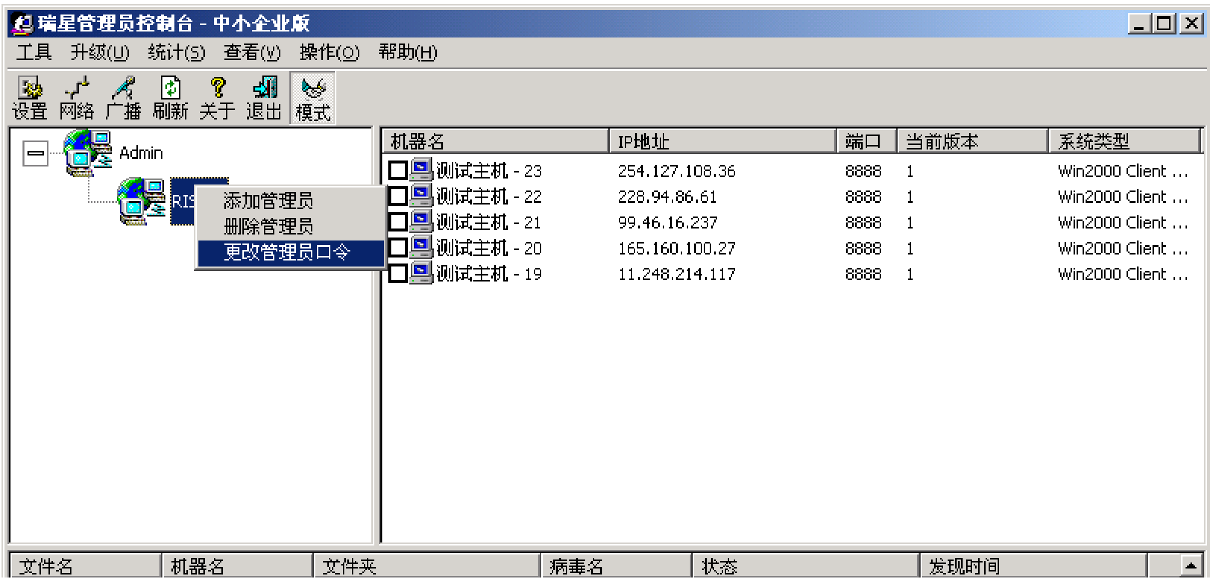


图 164

方法一：选定希望删除的管理员，点击鼠标右键选择【删除管理员】。

方法二：选定希望删除的管理员，点击菜单【操作】中的【删除管理员】项。

6.6 历史记录管理

历史记录管理是瑞星杀毒软件中小企业版的日志功能，其中记录了网络中计算机感染病毒的情况。管理员可以依据自己的需要察看网络计算机感染病毒的情况，分析和统计病毒的分布情况。

6.6.1 历史记录的启动

◆ 可以点击工具栏中的按钮打开【历史记录】。（如图 165）

◆ 在管理控制台打开的状态下可以通过快捷键【Ctrl+t】打开【历史记录】。

◆ 可以点击菜单【工具】中的【查看病毒警告历史记录】项，打开【历史记录】。

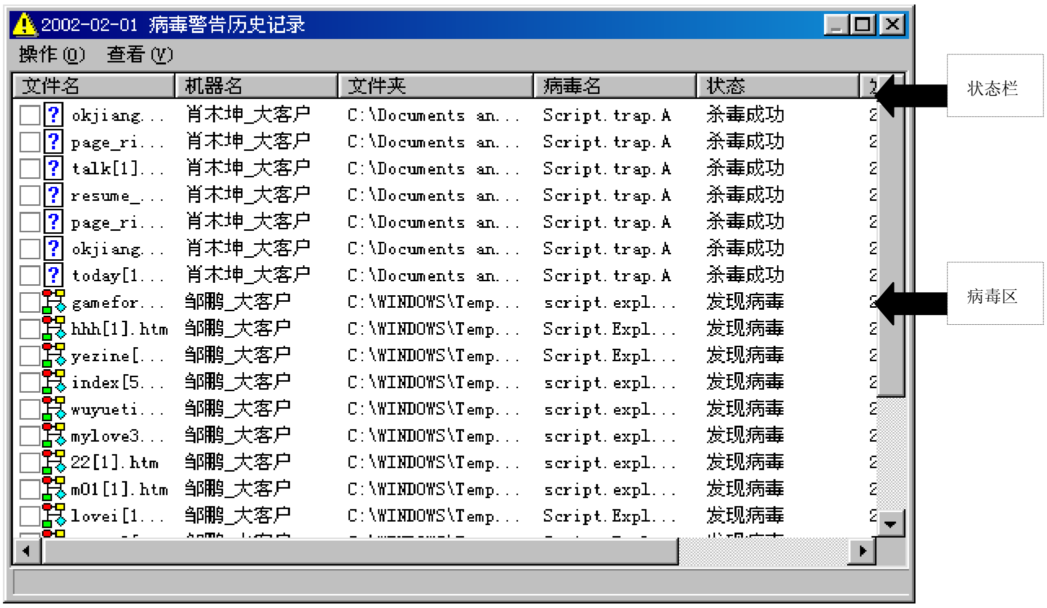


图 165

6.6.2 历史记录的操作

通过病毒历史记录的菜单进行相应的操作。（如图 166）



图 166

◆ 【操作】菜单：

单击【操作】菜单、打开历史记录。（如图 167）

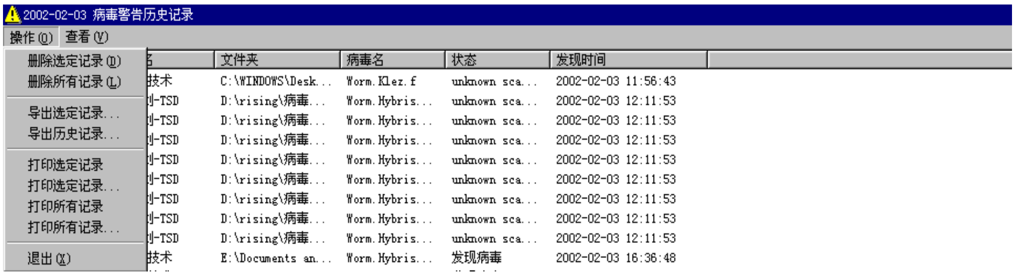


图 167

A）删除所选记录：单击【操作】菜单中的【删除所选记录】选项可以删除用户选定的历史记录信息。

B）删除所有记录：单击【操作】菜单中的【删除所有记录】，即可以将所有病毒警告历史记录删除。

C）导出选定记录：单击【操作】菜单中的【导出选定记录】，即可以将病毒信息备份到指定的文件中。（如图 168）

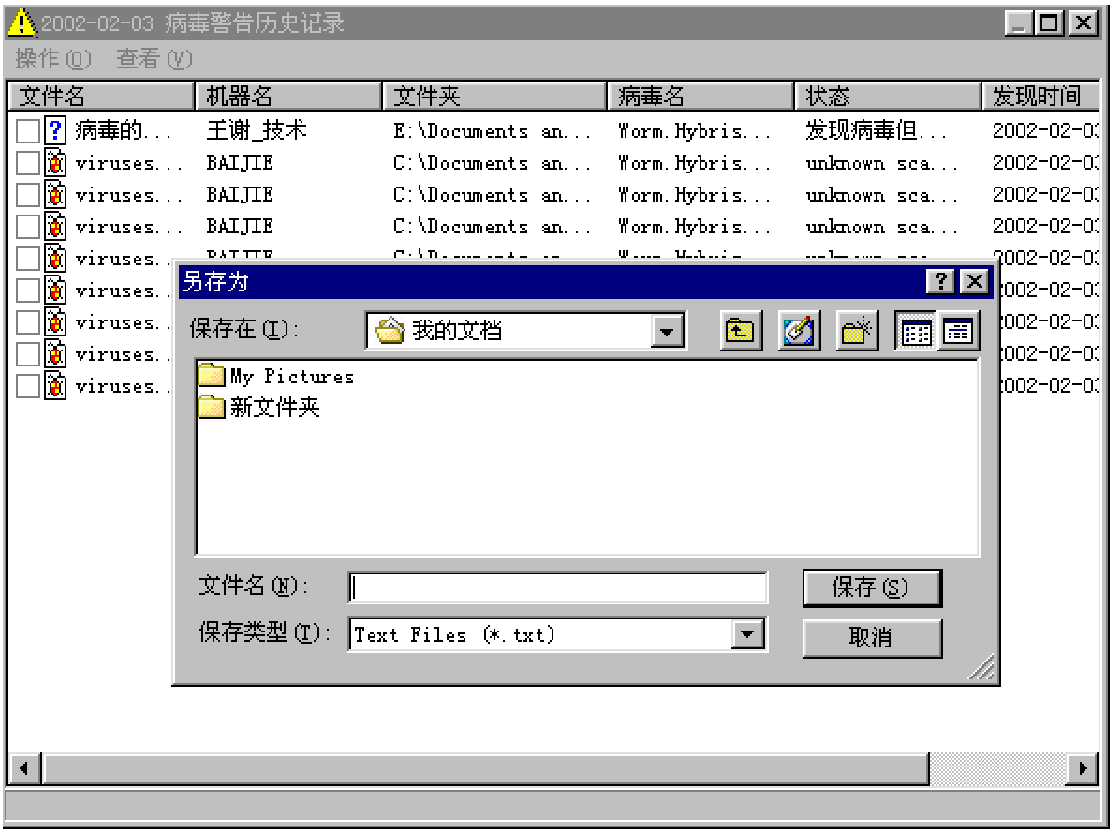


图 168

D）打印历史记录：单击【操作】菜单中打印历史记录的选项可以按照管理员的要求打印出病毒的历史信息。

◆ 【查看】菜单：

单击病毒警告历史记录的【查看】菜单项打开【查看】菜单。（如图 169）



图 169

A）看指定日期的记录：通过选择菜单中的查看选项可以查看任何一天的病毒历史记录。

B）过对【查看】菜单中【全选】,【全不选】和【反选】项的选择可以确定选中的历史记录信息。

C）通过点击【查看】菜单中的【文字统计报告】项，可以对感染病毒的计算机进行统计和分析。（如图 170）

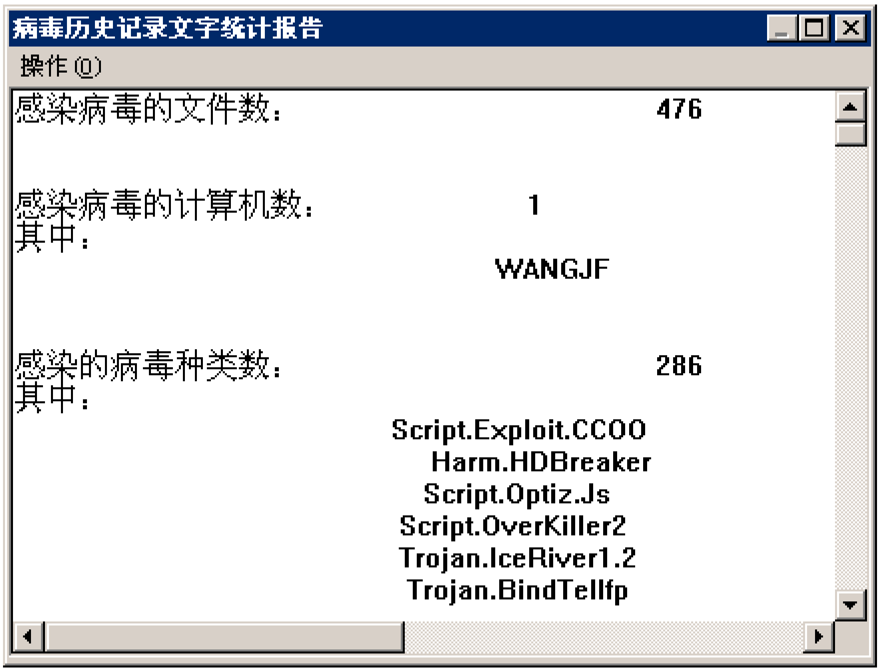


图 170

D）通过点击【查看】菜单中的【图形统计报告】项，可以更形象的得到计算机染毒情况的信息。（如图 171）

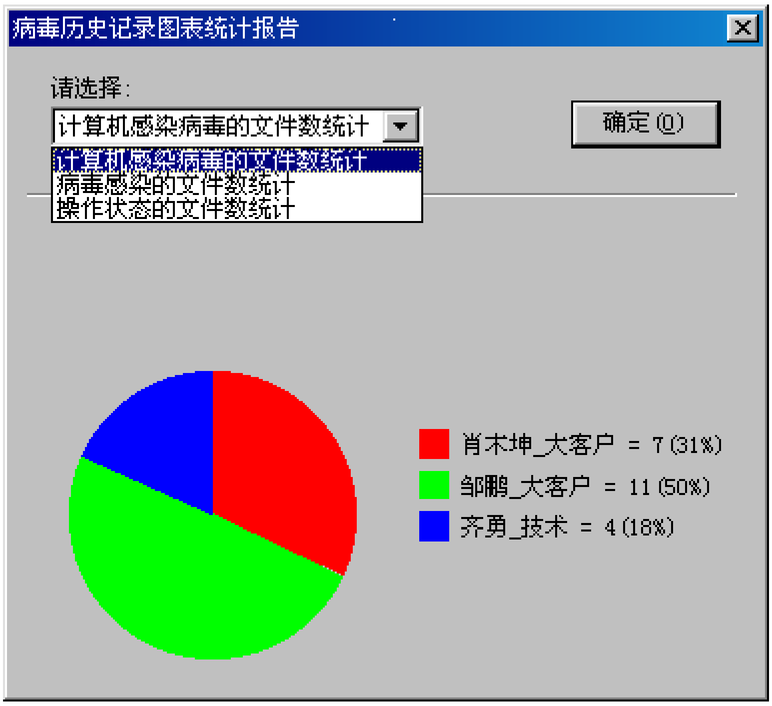


图171

6.7 其他

6.7.1 广播的应用

瑞星管理员管理控制台提供广播的功能。管理员可以通过管理控制台对所有或指定的客户端发布文本消息，实现了远程的病毒预警功能。此项功能实现了管理员对客户端的语言化交流，使得管理更加高效和合理。

◆　广播的应用

A）在机器列表栏选中需要接受广播的用户，单击【工具】菜单栏选定【发送广播消息】或者单击功能快捷按钮【广播】。（如图 172）

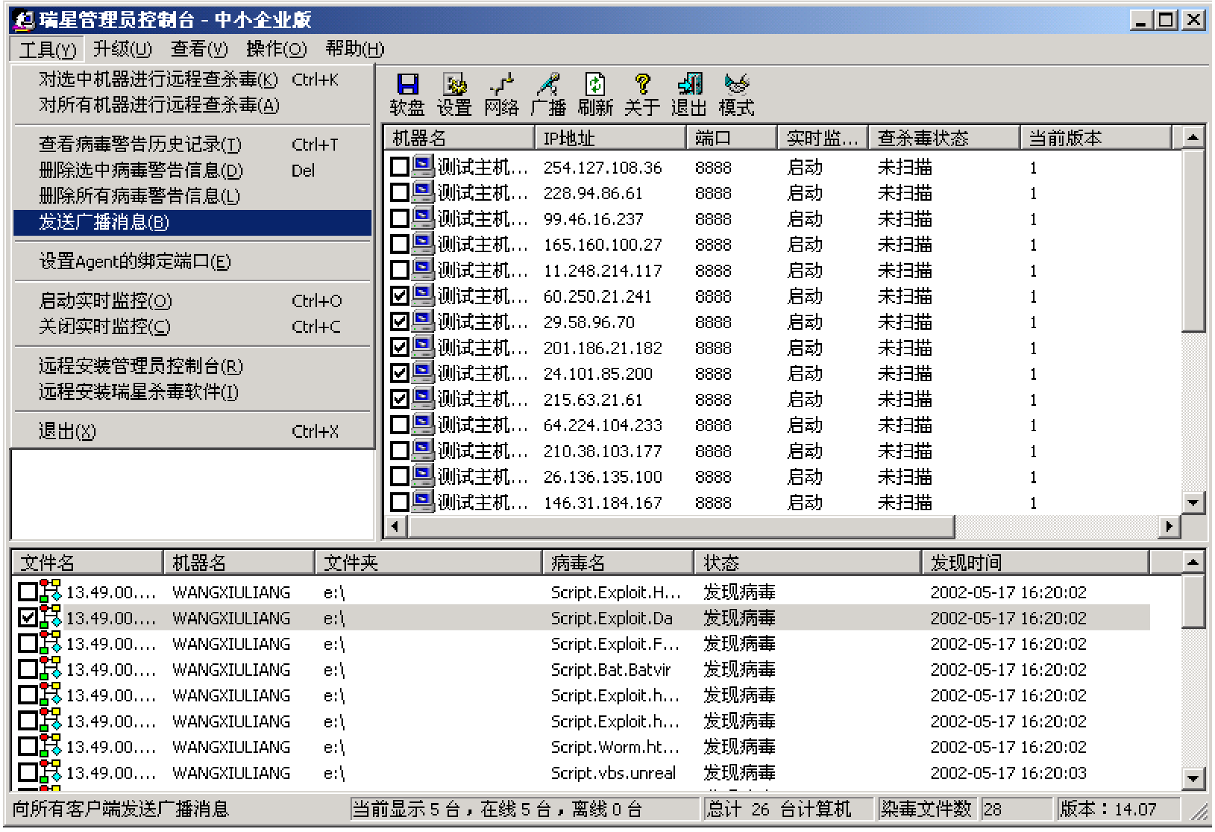


图 172

B）在弹出的【广播窗口】中输入文本信息，单击【发送】。（如图 173）



图 173

C）在目标客户端将出现【客户端服务程序】提示框，读取完消息后，单击【隐藏】按钮即可关闭该窗口。（如图 174）

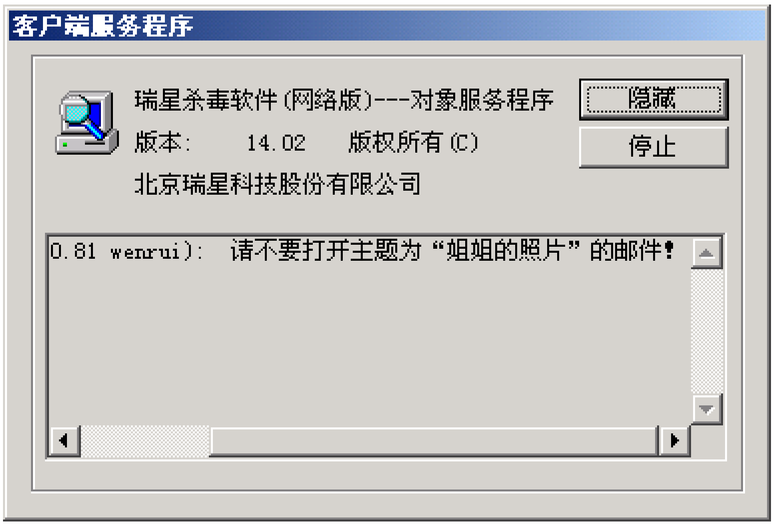


图 174

注意：当您不对接受广播的用户做出选定时，默认的是当前所有用户。

6.7.2 授权记数的释放

当瑞星客户端程序所在的机器发生诸如更换操作系统，更换 IP 地址等变化时，需要通过管理控制台程序去释放这类机器仍然占用的 License 记数。避免一台机器同时占用多个 License 记数。

◆ 操作过程

A）单击功能菜单项【操作】菜单，选择【更改到管理模式】或单击功能快捷按钮【模式】。（如图 175）

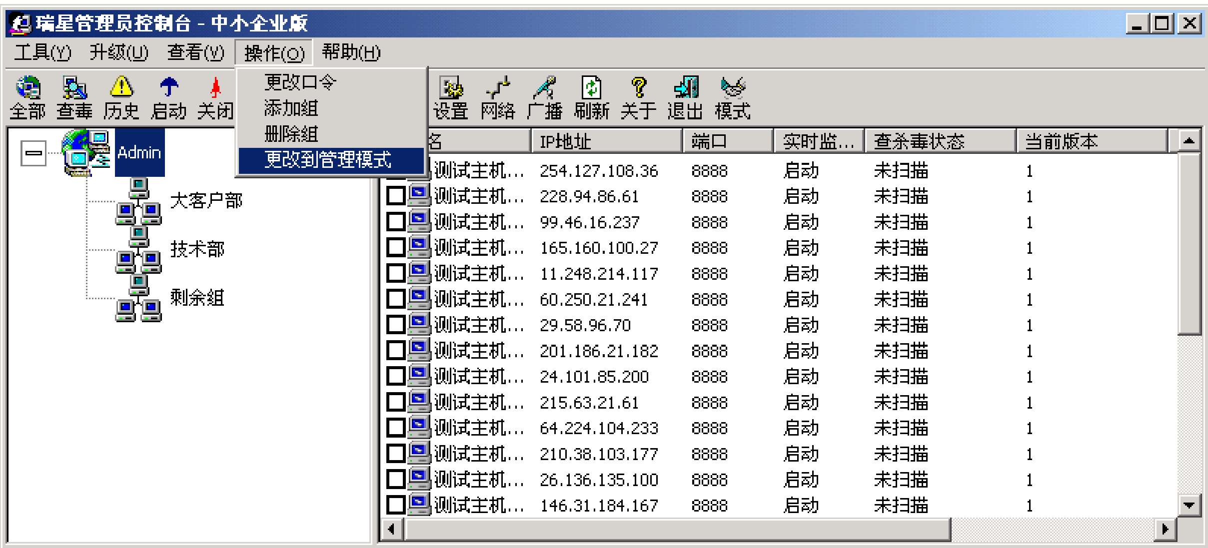


图 175

B）切换到模式状态下，选中需要释放的用户，单击鼠标右键，在弹出的菜单项中选择【删除所选机器】（如图 176）或者单击【工具】菜单，选中【删除所选机器】（如图 177）也可以实现相同的功能。

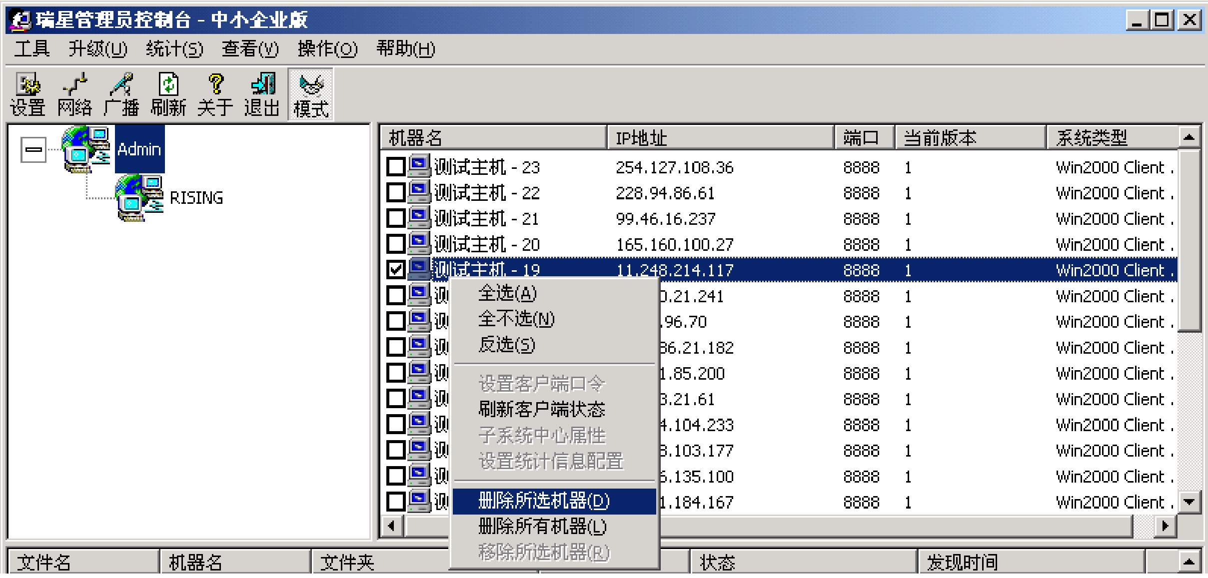


图 176

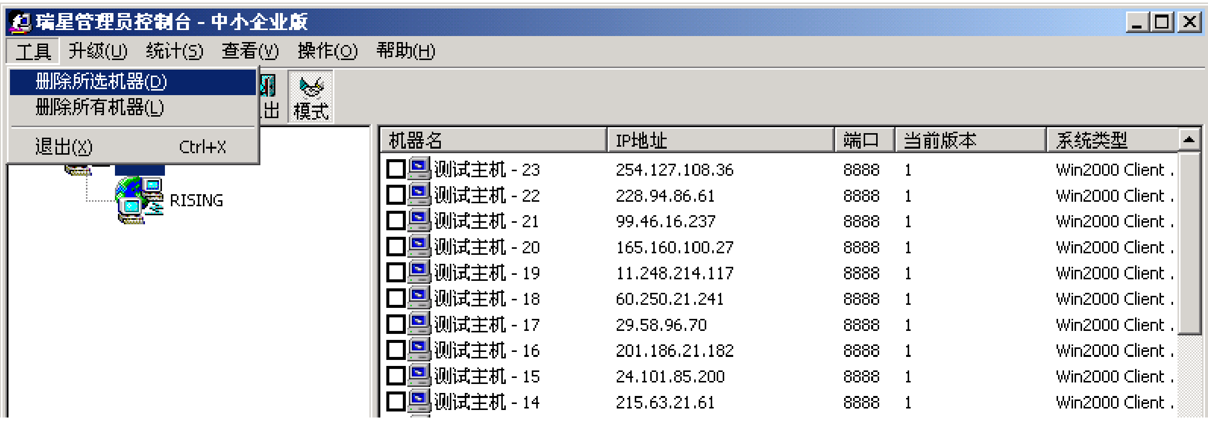


图 177

C）在弹出的【提示信息】对话框中单击【确定】，当前选定用户占用的 License 数即被释放。（如图 178）

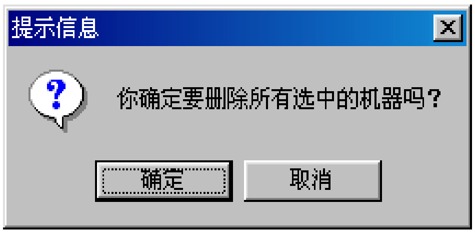


图 178

6.7.3 记数统计

管理员可以通过瑞星管理控制台程序查看瑞星杀毒软件【授权记数的使用情况】和【已注册机器的统计情况】。

◆ 应用过程

A）单击功能菜单项【操作】菜单，选择【更改到管理模式】或单击功能快捷按钮【模式】，切换到管理员管理模式状态下。（如图 179）

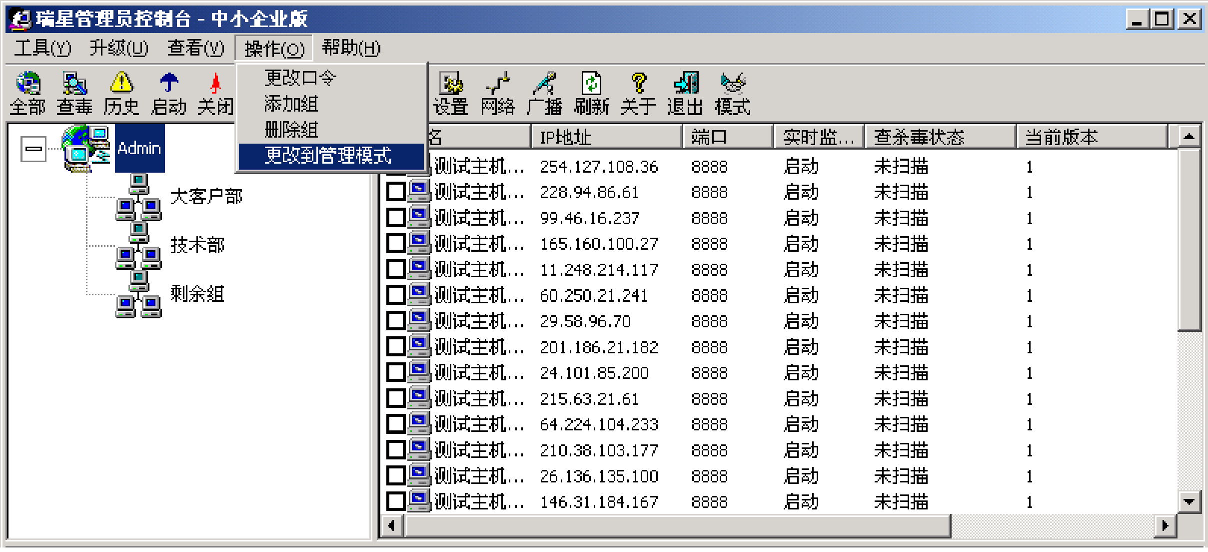


图 179

B）在管理员管理模式状态下，单击工具菜单栏【统计】按钮，在弹出的菜单项中选择【已注册机器的统计情况】。（如图 180）

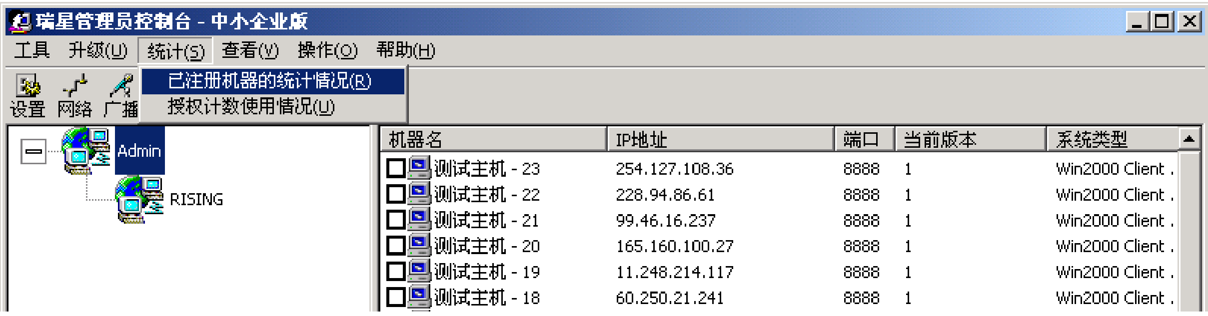


图 180

C）在弹出的对话框中显示了当前已注册用户的情况，单击【刷新】按钮，获取最新情况。（如图 181）

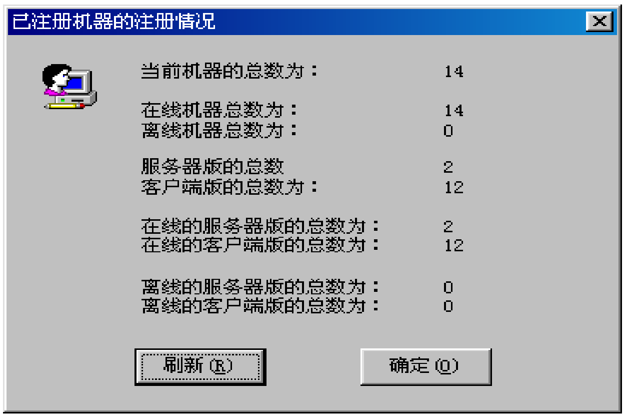


图 181

D）选择【授权记数使用情况】项，在弹出的对话框中可以获取授权记数使用情况的具体信息。（如

图 182）

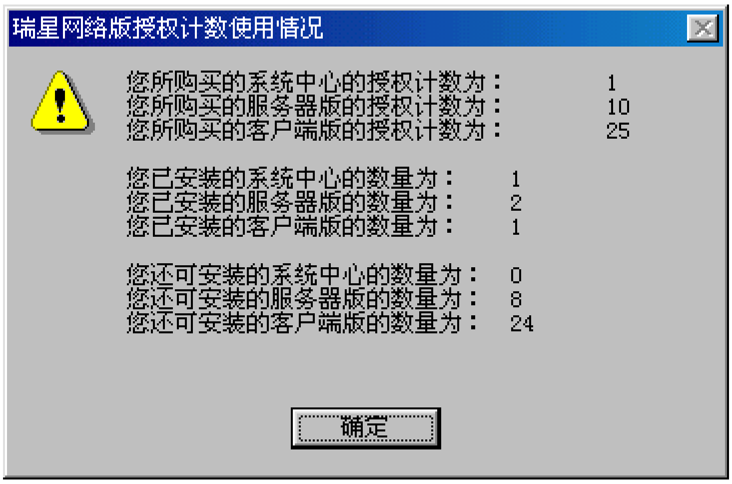


图 182

6.7.4 设置 Agent 绑定端口

为了给工作在系统中心的瑞星后台程序指定其使用的端口号。在需要的时候，管理员可以在(7273~7282)之间为其指定一个端口号，后台程序会在这个范围以内随机的自动绑定。

◆ 应用过程

A)启动瑞星管理员管理控制台程序，单击功能菜单【工具】，选定【设置 Agent 的绑定端口】项。（如图 183）

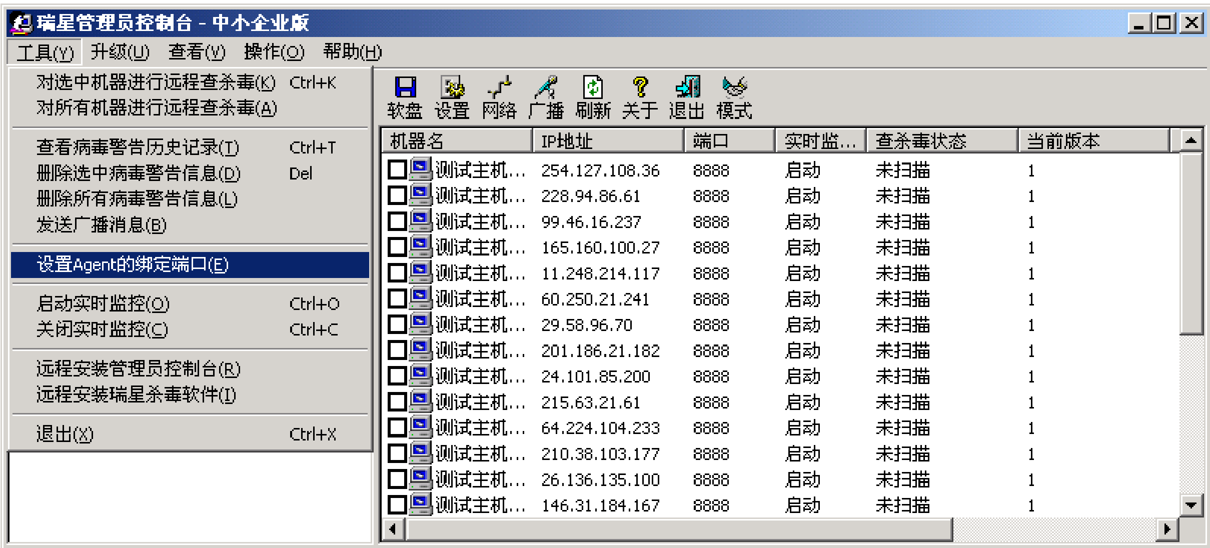


图 183

B)在弹出的对话框中单击下拉按钮【▼】选定您需要设定的端口号。（如图 184）

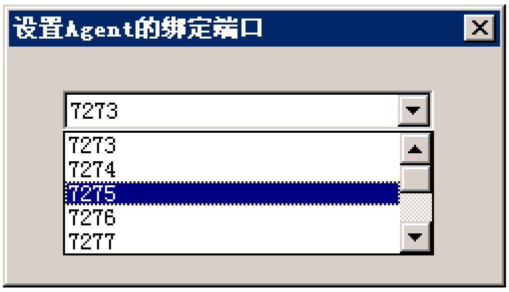


图 184

C)单击【确定】按钮，完成设置 Agent 的绑定端口的操作。（如图 185）



图 185

提示：网络版客户端状态（包括时实监控的状态，查杀状态，在线情况等）在管理控制台【计算机列表栏】的实时显示，可以使管理员主动掌握最新的客户端状态，第一时间判断客户端的实际情况。

连接状态的三种情况为【激活】、【未激活】和【未响应】:

A）激活：客户端程序处于正常工作状态，此时管理控制台发出的所有指令都将被客户端执行。

B）未激活：客户端处于关机或异常终止状态，此时无法对管理控制台发出的命令做出响应。

C）未响应：对于由网络原因而临时不在线的客户，管理控制台程序给出了一个【中间状态】的处理，既【未响应】状态。

第七章 升级

当安装网络版杀毒软件后，升级工作应该是您首要进行的重要工作。杀毒软件的特性决定了升级操作所处的重要地位。能够方便的利用互联网实时更新软件的版本，自动分发升级程序到客户端是瑞星软件升级系统的特色。

提示：强烈建议您把您的瑞星杀毒软件升级到最新版本并进行全网杀毒以保障您目前的网络处于健康的状况。

7.1 网络配置

在进行软件升级之前，请务必配置好网络的设置以保障能够及时顺利进行软件版本的更新升级。

启动【瑞星管理员管理控制台】，点击【网络】按钮或者升级菜单中的【网络设置】项即可进入瑞星杀毒软件升级网络设置，瑞星[中小企业版]提供 3 种网络连接方式，具体操作请参照 windows 操作系统连接互连网方法，这里只做简单介绍。

7.1.1 局域网（LAN）或专线上网

如果安装瑞星系统中心的服务器使用直接连接 internet 的方式，请选择此项。(如图 186)

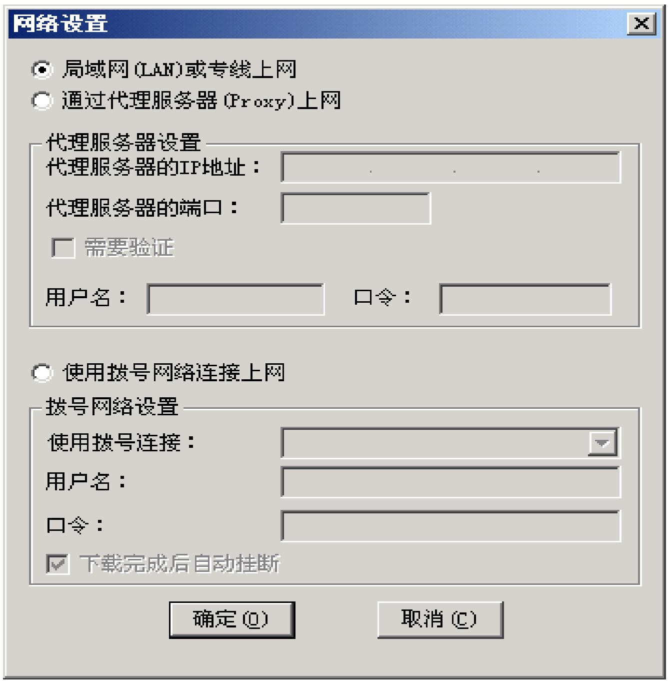


图 186

7.1.2 通过代理服务器（Proxy）上网

如果安装瑞星杀毒软件[中小企业版]系统中心的服务器是通过代理服务器连接 Internet，请选择此项。网络设置会自动读取使用代理服务器的 IP 地址和端口号。如需要身份验证，请选中【需要验证】，并且输入用户名和密码。(如图 187)



图 187

注意：如果【网络设置】没有检测到代理服务器的 IP 地址和端口号，说明代理服务器的设置不正确，请您手工输入正确的 IP 地址和端口号。

7.1.3 使用拨号方式连接上网

如果安装瑞星杀毒软件[中小企业版]系统中心的服务器使用调制解调器，ISDN 或其他拨号方式连接 internet，请选择此项。【网络设置】同样会自动检测到拨号设置。如图 188，点击【确定】按钮，网络设置完毕。

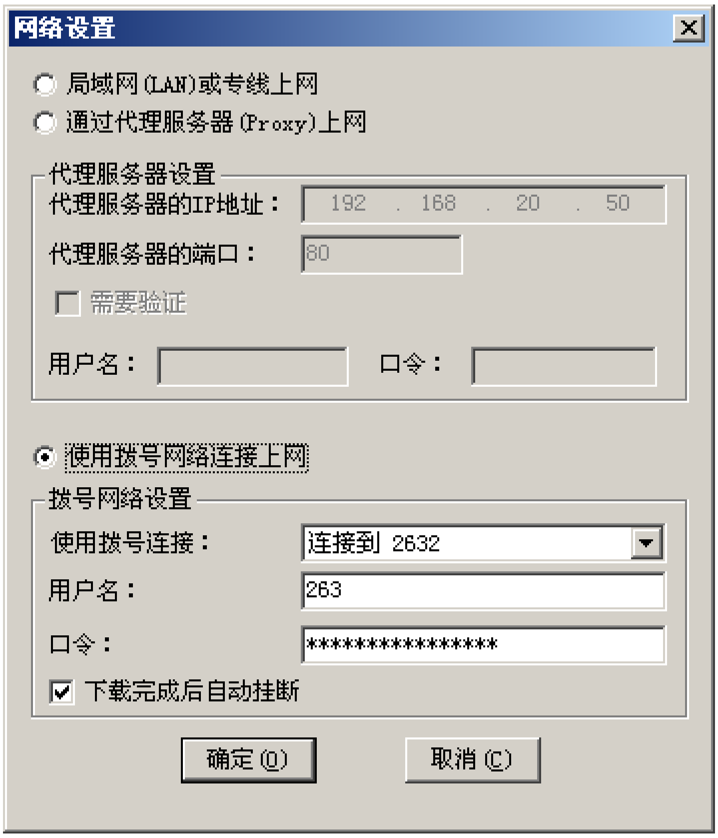


图 188

7.2 升级设置

依据您的实际工作情况和网络状况，可以在【升级设置】中设定好升级的方式和时间进行版本的升级。

7.2.1 启动

瑞星杀毒软件[中小企业版]的升级设置的窗口可以通过【瑞星管理员管理控制台】上的【设置】按钮或【升级】菜单里的【升级设置】来打开。

7.2.2 升级方式

在升级设置中，瑞星网络版杀毒软件提供了如下 3 种升级方式。（如图 189）



图 189

◆ 自动下载，自动升级：

“自动下载，自动升级”的特点是升级用户可以在指定的时间范围内进行版本升级。升级的整个过程无需用户的人工介入。

◆ 自动下载，手动升级：

对于网络安全性能要求较高的用户建议采用这种方式，自动下载升级程序后，可以在用户方便的时间进行手动升级。

◆ 不使用自动设置：

对于网络连接不方便或安装“瑞星系统中心”的服务器不能连接 Internet 的用户建议采用这种方式。

7.2.3 定时方式

◆ 【升级设置】提供了定时启动【自动升级】的设置，用户可根据自身情况定时升级。(建议：定时方式：每日，星期：星期日)(如图 189)

◆ 当完成上述设置后，瑞星杀毒软件[中小企业版]自动依据设定的时间进行版本升级。

7.3 升级操作

本节为您介绍了不同的升级方式和方法的升级的过程，您可以据此来判断您的系统是否升级正常。

7.3.1 自动下载，自动升级

◆ 从瑞星网站下载升级文件到系统中心。（如图 190、图 191）

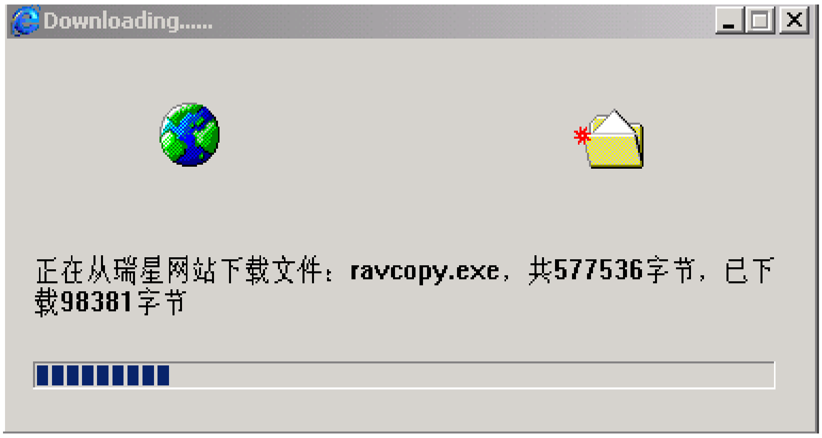


图 190

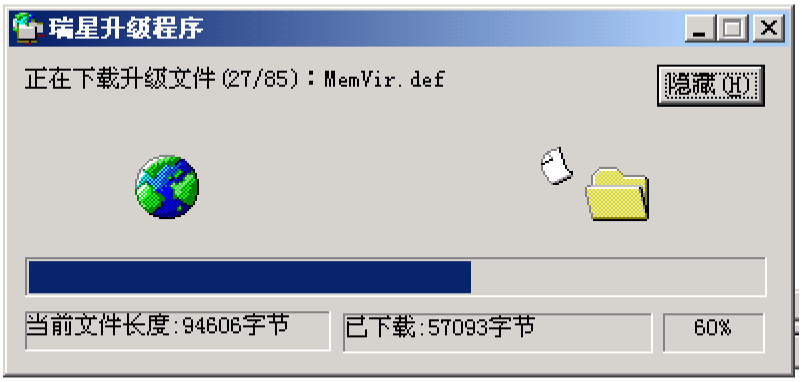


图 191

◆ 下载文件完成后，瑞星自动升级程序进行文件的更新。（如图 192）



图 192

◆ 更新完文件后，瑞星自动升级程序会给您升级成功的提示。（如图 193）

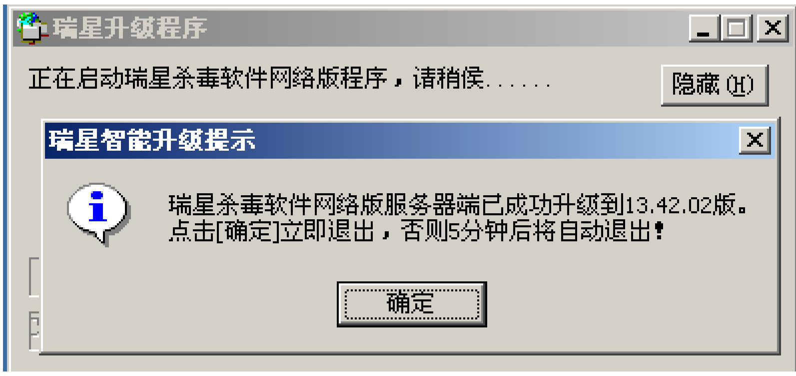


图 193

7.3.2 自动下载，手动升级

◆ 如果您在“升级设置”中选择的是【自动下载，手动升级】，当进行升级时，瑞星自动升级程序会自动和瑞星网站进行连接并下载手动升级程序。（如图 194）

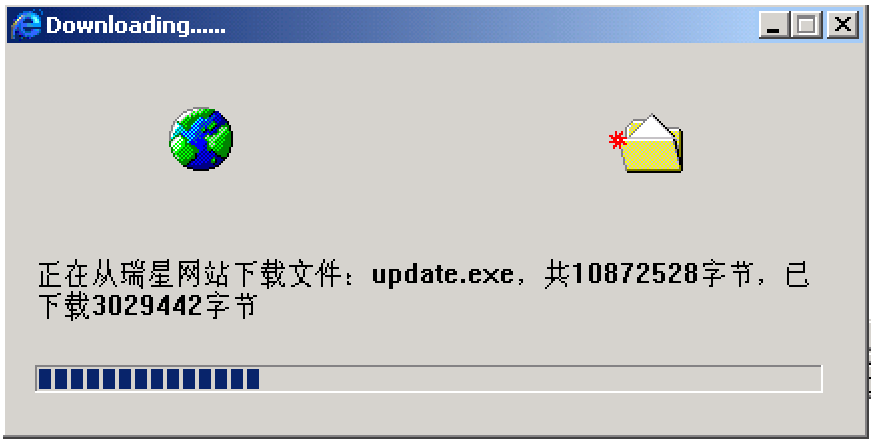


图 194

◆ 升级程序下载完毕。（如图 195）。您可以通过【手动升级】的方式进行升级。（有关详情请参见【手动升级】）

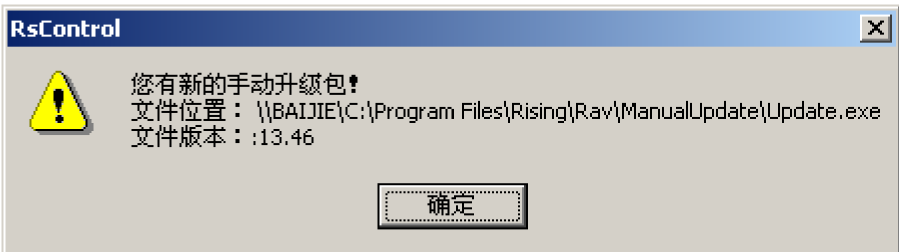


图 195

7.3.3 不使用自动设置的升级方式

如果您在【升级设置】选项中选择了【不使用自动设置】项，那么可采用以下两种升级方式。

◆ 立即升级

点击【瑞星管理员管理控制台】的【立即】按钮或【升级】菜单里的【立即升级】，瑞星自动升级程序会连接瑞星网站自动升级。单击【确定】完成。(如图 196)



图 196

◆ 手动升级

对于不采用【自动升级】方式的用户，可以采用【手动升级】的方式进行软件的升级。点击管理控制台【手动】按钮或【升级】菜单里的【手动升级】，在弹出的【打开】对话框中选中已下载的升级程序包。单击【打开】按钮即可进行升级。(如图 197)

A)如何得到手动升级包：

得到瑞星手动升级包的直接方法是到瑞星网站（WWW.RISING.COM.CN）下载升级程序。输入您的产品 ID 确定后便可以下载升级包了。

产品 ID 是您购买产品后得到的授权标志，ID 是您产品对应的标示，一套产品只有一个 ID 号，因此请妥善保管您的产品 ID 号。

提示：请立即正确填写‘用户注册卡’并邮寄回瑞星技术服务部。瑞星公司将提供给您有 ID 号的产品授权书。

注意：对于同一个版本的升级程序，允许您进行五次升级程序下载。

B)手动升级过程：

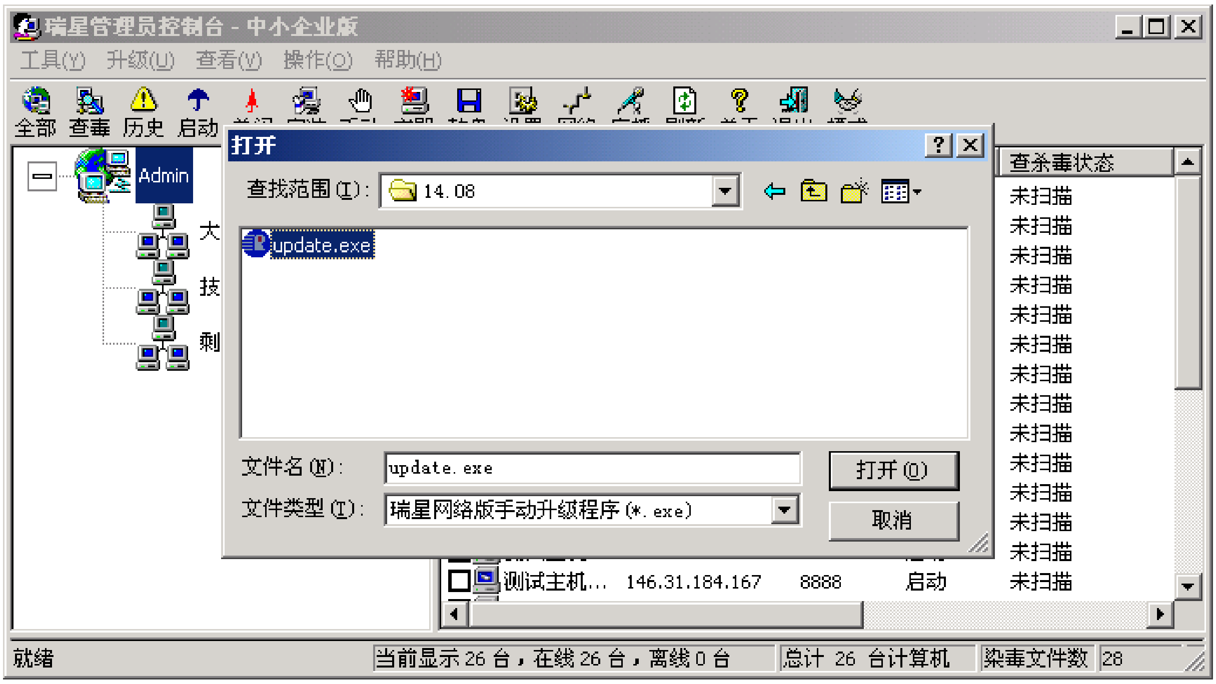


图 197

手动升级程序开始运行。（如图 198）

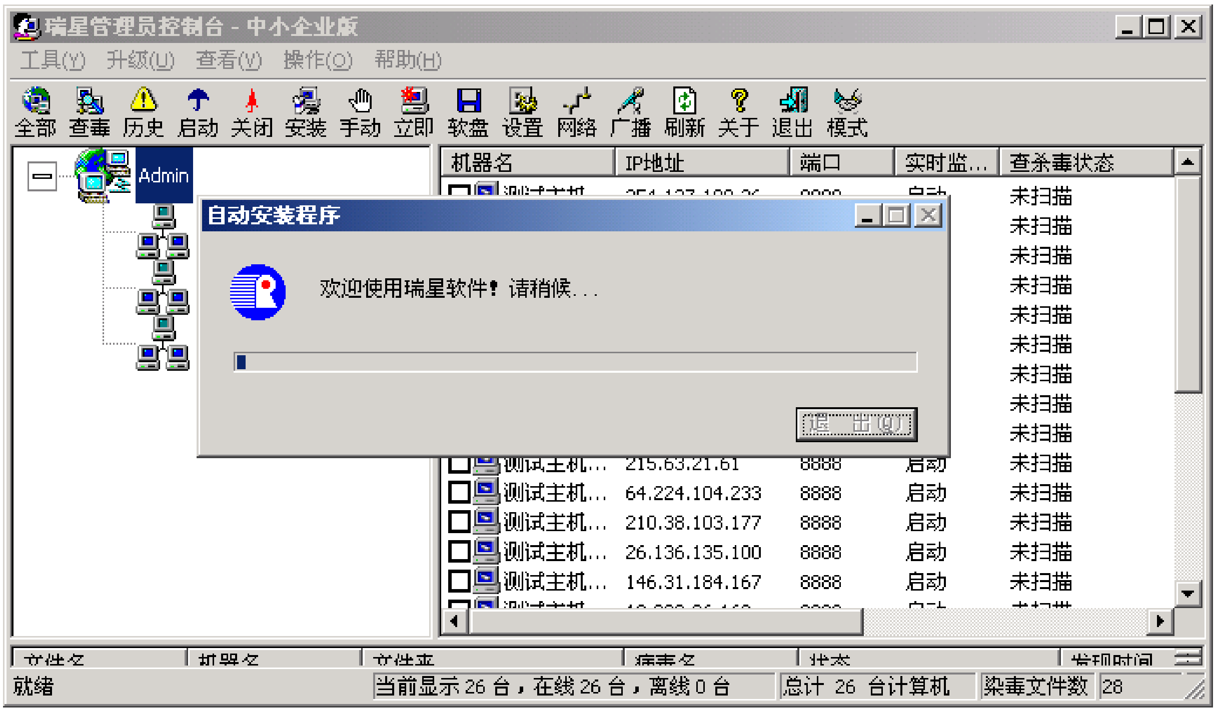


图 198

文件的更新复制过程如图 199、图 200。



图 199

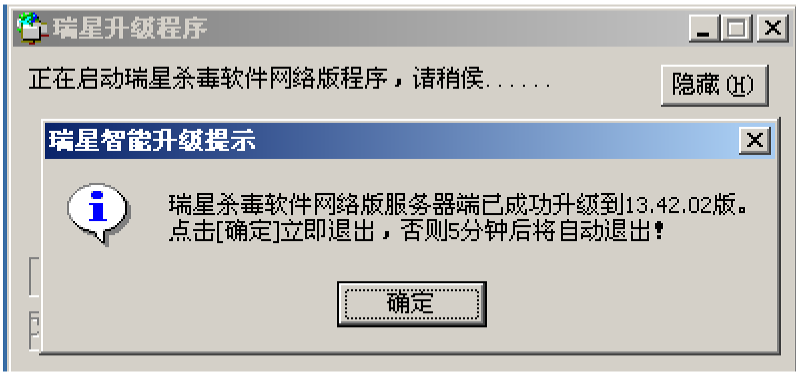


图 200

注意：无论采用【自动升级】或是【手动升级】，只能在安装瑞星系统中心的服务器上进行（以下简称系统中心），待系统中心升级成功后，客户端会自动比照系统中心升级。

注意：手动升级不能直接运行升级包，必须按照瑞星指定的升级方法进行升级。

7.4 升级瑞星 DOS 软盘

升级瑞星 DOS 软盘有两种方式，在【瑞星管理员管理控制台】上直接升级或在任意已成功安装瑞星杀毒软件的客户机上进行软件的升级。

7.4.1 在【瑞星管理员管理控制台】上升级瑞星 DOS 软盘

启动【瑞星管理员管理控制台】，点击【软盘】按钮，如图 201，启动进入【制作瑞星 DOS 盘】界面，点击【下一步】，

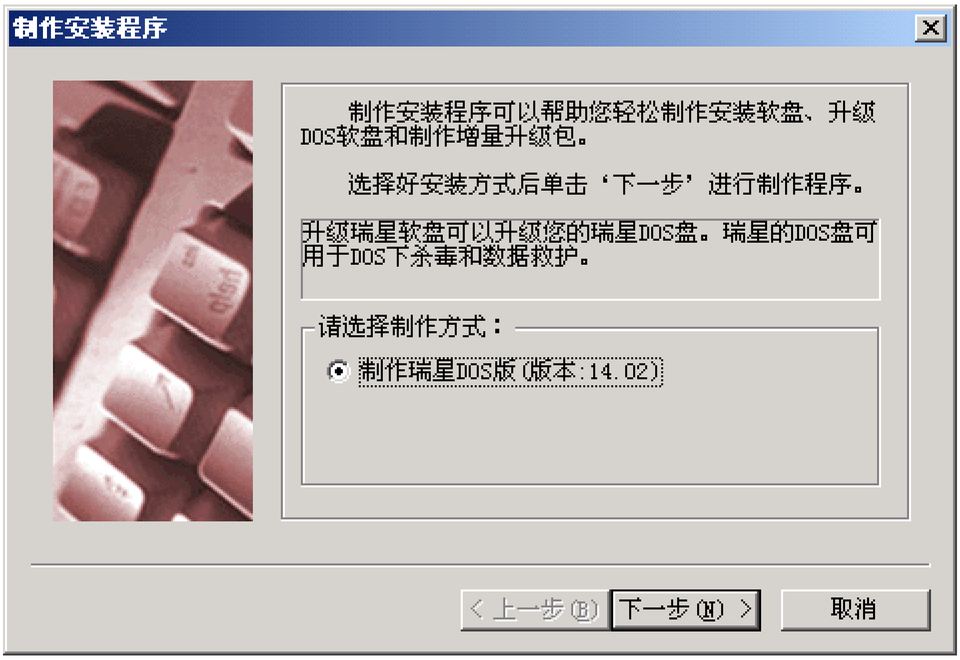


图 201

根据提示打开 A 号盘的写保护并插入 A 驱动器，如图 202，点击【下一步】，

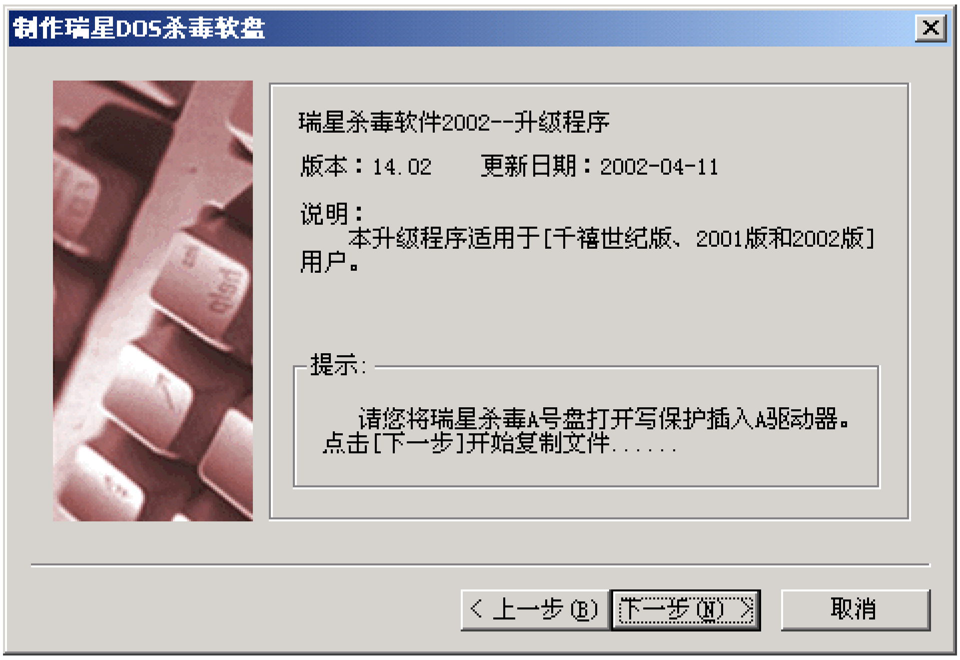


图 202

A 盘升级更新文件开始，如图 203：



图 203

当 A 盘升级完毕时（如图 204），根据提示打开 B 号软盘的写保护并插入 A 驱动器，点击【确定】按钮，继续升级 DOS 盘第二张磁盘，升级完毕时（如图 205）点击【完成】即可完成 DOS 盘升级。



图 204



图 205

注意：**DOS 盘升级完毕时应及时的把软盘写保护关闭，以防止感染引导区病毒。**

7.4.2 在客户机上升级瑞星 DOS 软盘

打开瑞星主程序，（如图 206）点击【工具】菜单里的【制作安装盘】，会出现软盘升级提示（如图 201），您可以依照 7.4.1 小节介绍的升级方法进行升级。（详细的升级过程参见 7.4.1）。



图 206

附录：使用过程中的故障问题解决

✧ 在安装网络版杀毒软件时，系统提示【系统初使化失败】而无法继续安装。
解决：请您运行瑞星网络版安装光盘中 tools 目录中的安装程序，安装结束后重新启动计算机。再次安装瑞星杀毒软件。

✧ 升级过程发生意外，升级失败。
解决：A、确定您是否采用的正确的升级方法。B、如果是手动升级，确定升级包下载正确。C、如果是自动升级确定网络设置是否正确。D、及时和瑞星公司技术部取得联系。

✧ 软盘引导时无法进入杀毒程序。
解决：软盘物理损坏或者是软盘的加密点丢失。请和瑞星公司联系换盘事宜。

✧ 系统报告【授权记数超出，请购买更多授权】。
解决：确定安装瑞星杀毒软件的服务器端和客户端是否超出购买的授权，否则，请和瑞星公司技术部联系购买更多的产品授权。

✧ 安装结束，控制台打开时系统提示【Agent 端口绑定失败】。
解决：此问题的出现是由于系统的某个程序占用了瑞星代理程序的端口号。可以通过管理控制台改变 Agent 的端口设定解决此问题。

✧ 在安装系统中心时，安装程序总是提示【安装服务器】端杀毒软件。
解决：确定您是否安装过瑞星网络版杀毒软件，如果在同一网段中存在另一个系统中心，请把另一个系统中心卸载后再安装新的系统中心。

✧ 客户端或者服务器端的计算机在系统中心的状态为【未激活】。
解决：A)确定未激活的计算机未关机。B)请确定该计算机和系统中心所在服务器可以相互通讯。